



RADIO FREQUENCY BASED  
PROGRAMMABLE LOGIC CONTROLLER  
ANOMALY DETECTION

DISSERTATION

Samuel J. Stone, Capt, USAF

AFIT-ENG-DS-13-S-05

DEPARTMENT OF THE AIR FORCE  
AIR UNIVERSITY

***AIR FORCE INSTITUTE OF TECHNOLOGY***

Wright Patterson Air Force Base, Ohio

DISTRIBUTION STATEMENT A.  
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

The views expressed in this dissertation are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.



AFIT-ENG-DS-13-S-05

RADIO FREQUENCY BASED  
PROGRAMMABLE LOGIC CONTROLLER  
ANOMALY DETECTION

DISSERTATION

Presented to the Faculty of the  
Graduate School of Engineering and Management  
of the Air Force Institute of Technology  
Air University

In Partial Fulfillment of the  
Requirements for the Degree of  
Doctor of Philosophy

Samuel J. Stone, B.S.C.E., M.S.E.E.  
Capt, USAF

September 2013

**DISTRIBUTION STATEMENT A.**  
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.


The views expressed in this dissertation are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

RADIO FREQUENCY BASED  
PROGRAMMABLE LOGIC CONTROLLER  
ANOMALY DETECTION

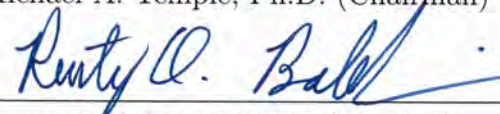
Samuel J. Stone, B.S.C.E., M.S.E.E.

Capt, USAF

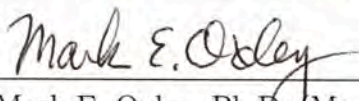
Approved:

  
\_\_\_\_\_  
Michael A. Temple, Ph.D. (Chairman)

15 Aug 13  
Date


  
\_\_\_\_\_  
Rusty O. Baldwin, Ph.D. (Member)

15 Aug 13  
Date

  
\_\_\_\_\_  
Mark E. Oxley, Ph.D. (Member)

15 Aug 2013  
Date

Accepted:

  
\_\_\_\_\_  
HEIDI R. RIES, Ph.D.  
Interim Dean, Graduate School of Engineering  
and Management

5 Sep 2013  
Date

*First and foremost, I want to thank the Lord, Jesus Christ for the opportunities He has blessed me with. Without Him, none of this would be possible.*

*To my wife and children, You've been instrumental in helping me get through this. I could not have done this without your support, patience, love and understanding.*

*To my parents and grandparents, Thank you for setting my path early. The values and motivations instilled through my youth have guided me to this point.*

*To my Father-in-law and Mother-in-Law, Thank you for hanging with me and keeping me motivated through the thick and thin.*

## *Acknowledgements*

Special thanks to my advisor Dr. Michael Temple. Your extensive knowledge in the field and ability to keep me focused are very much appreciated. You've done an amazing job turning this "bit-head" into slightly less of a "bit-head". I couldn't have wished for a better advisor! I would also like to thank my research committee, Dr. Baldwin and Dr. Oxley for the support. You've done an incredible job of representing the breadth of knowledge maintained at AFIT.

Samuel J. Stone

## Table of Contents

	Page
Acknowledgements . . . . .	v
List of Figures . . . . .	ix
List of Tables . . . . .	xi
List of Abbreviations . . . . .	xii
Abstract . . . . .	xv
1. Introduction . . . . .	1
1.1 Operational Motivation . . . . .	1
1.1.1 Software-Based Vulnerabilities . . . . .	5
1.1.2 Hardware-Based Vulnerabilities . . . . .	7
1.2 Technical Motivation . . . . .	8
1.2.1 Emission Collection . . . . .	10
1.2.2 Fingerprint Generation . . . . .	12
1.2.3 Device Classification . . . . .	12
1.2.4 Device ID Verification . . . . .	13
1.2.5 Correlation and Matched Filtering . . . . .	13
1.3 Research Contributions . . . . .	14
1.4 Document Organization . . . . .	15
2. Background . . . . .	17
2.1 SCADA and ICS Applications . . . . .	17
2.1.1 Programmable Logic Controller (PLC) . . . . .	18
2.1.2 Ladder Logic Program (LLP) . . . . .	19
2.1.3 Human Machine Interface (HMI) . . . . .	20
2.2 SCADA and ICS Vulnerabilities . . . . .	21
2.3 RF Emission Collection . . . . .	22
2.3.1 Near-Field RF Probe . . . . .	25
2.3.2 Digital Sampling . . . . .	25
2.4 Post-Collection Processing . . . . .	27
2.4.1 Correlation . . . . .	27
2.4.2 Hilbert Transform . . . . .	28
2.5 Verification-Based Discrimination . . . . .	29
2.5.1 ROC Performance Assessment . . . . .	30

	Page
3. Methodology . . . . .	31
3.1 PLC Device Description . . . . .	32
3.2 PLC Operating Conditions . . . . .	34
3.2.1 Ladder Logic Program: $N_{OP}=5$ . . . . .	34
3.2.2 Ladder Logic Program: $N_{OP}=10$ . . . . .	35
3.3 CBAD Processing Overview . . . . .	35
3.4 RF Emission Processing . . . . .	37
3.4.1 Collection and Sampling . . . . .	38
3.4.2 PLC Mainboard Mounting . . . . .	39
3.4.3 RF Near-Field Probe Placement . . . . .	40
3.4.4 PLC LLP Triggering . . . . .	43
3.5 Post-Collection Processing . . . . .	43
3.5.1 Down-Conversion and Bandpass Filtering . . . . .	44
3.5.2 Sub-Sampling/Proper Decimation . . . . .	45
3.5.3 Signal-to-Noise Ratio Scaling . . . . .	45
3.6 Sequence Transformation . . . . .	48
3.6.1 Hilbert Transform . . . . .	48
3.6.2 RF-DNA Transform . . . . .	49
3.7 Region of Interest Selection . . . . .	52
3.8 CBAD Processing . . . . .	58
3.8.1 Testing and Training Set Generation . . . . .	58
3.8.2 Reference Sequence $x_R[n]$ Generation . . . . .	60
3.8.3 Test Statistic $z_V$ Generation . . . . .	61
3.8.4 Verification Threshold Determination . . . . .	61
3.8.5 Anomalous vs. Normal Declaration . . . . .	62
3.9 LLP Operation-by-Operation Processing . . . . .	62
3.10 Performance Evaluation . . . . .	64
3.10.1 Performance Curves . . . . .	64
3.10.2 CBAD Statistical PMFs . . . . .	65
3.10.3 ROC Curve Assessment . . . . .	65
3.11 GRLVQI Processing . . . . .	66
4. Results . . . . .	68
4.1 PLC Response Sequences . . . . .	68
4.2 Performance Evaluation Criteria . . . . .	69
4.3 Software Anomaly Detection: TD Sequences . . . . .	70
4.3.1 Single Device, $N_B=1$ , $N_{Op}=5$ . . . . .	70
4.3.2 Single Device, $N_B=60$ , $N_{Op}=5$ . . . . .	71
4.4 Software Anomaly Detection: RF-DNA Sequences . . . . .	74

	Page
4.4.1 Single Device, $N_B=60$ , $N_{Op}=5$ . . . . .	76
4.5 Software Anomaly Detection: Hilbert Sequences . . . . .	78
4.5.1 Single Device, $N_B=60$ , $N_{Op}=5$ . . . . .	79
4.5.2 Ten Devices, $N_B=1000$ , $N_{Op}=10$ . . . . .	81
4.6 Hardware Component Discrimination . . . . .	86
4.6.1 GRLVQI Verification: TD Sequences . . . . .	87
4.6.2 GRLVQI Verification: CD Sequences . . . . .	90
5. Conclusion . . . . .	95
5.1 Research Summary . . . . .	95
5.2 CBAD Software Anomaly Detection . . . . .	97
5.3 GRLVQI Hardware Component Discrimination . . . . .	100
5.4 Future Research Recommendations . . . . .	102
5.5 Sponsor Acknowledgment . . . . .	104
Bibliography . . . . .	105



## *List of Figures*

Figure		Page
1.1	OSI Network Model . . . . .	4
2.1	Allen Bradley RSLogix® LLP Example . . . . .	19
3.1	Device Spectral Intensity Plots . . . . .	33
3.2	Normal and Anomalous Ladder Logic Programs . . . . .	36
3.3	CBAD Process Overview . . . . .	37
3.4	Representative Normalized PSD . . . . .	38
3.5	Physical Low Pass Filter Frequency Response . . . . .	39
3.6	Collection Table Configuration . . . . .	40
3.7	Course Probe Placement Markings . . . . .	41
3.8	Digital Band Pass Filter Frequency Response . . . . .	44
3.9	Digital Low Pass Filter Frequency Response . . . . .	46
3.10	Representative Collected Waveforms . . . . .	50
3.11	RF-DNA Fingerprint Diagram . . . . .	53
3.12	Representative Collected Scan Waveform . . . . .	54
3.13	Emissions for $N_{OP}=10$ Operation LLPs . . . . .	63
3.14	Operation-by-Operation CBAD Process Diagram . . . . .	64
4.1	$SNR$ vs. $TADR$ for TD Sequence, $N_B=1$ , $N_{OP}=5$ . . . . .	71
4.2	ROC curve for TD Sequence, $N_B=1$ , $N_{OP}=5$ . . . . .	72
4.3	$SNR$ vs. $TADR$ for TD Sequence, $N_B=60$ , $N_{OP}=5$ . . . . .	73
4.4	ROC Curve for TD Sequence, $N_B=60$ , $N_{OP}=5$ . . . . .	74
4.5	PMF for TD Sequence, $N_B=60$ , $N_{OP}=5$ . . . . .	75
4.6	$SNR$ vs. $TADR$ for RF-DNA Sequence, $N_B=60$ , $N_{OP}=5$ . . . . .	77
4.7	ROC Curve for RF-DNA Sequence, $N_B=60$ , $N_{OP}=5$ . . . . .	78
4.8	$SNR$ vs. $TADR$ for RF-DNA Sequence, $N_B=60$ , $N_{OP}=5$ . . . . .	79
4.9	ROC Curve for RF-DNA Sequence, $N_B=60$ , $N_{OP}=5$ . . . . .	80

Figure		Page
4.10	$SNR$ vs. $TADR$ for Hilbert Sequence, $N_B=60$ , $N_{OP}=5$ . . .	81
4.11	ROC Curve for Hilbert Sequence, $N_B=60$ , $N_{OP}=5$ . . . . .	82
4.12	$SNR$ vs. $TADR$ for Hilbert Sequence, $N_B=1000$ , $N_{OP}=10$ .	83
4.13	ROC Curve for Hilbert Sequence, $N_B=1000$ , $N_{OP}=10$ . . . .	84
4.14	$SNR$ vs. $TADR$ for Operation-by-Operation Hilbert Sequence, $N_B=1000$ , $N_{OP}=10$ . . . . .	85
4.15	ROC Curve for Operation-by-Operation Hilbert Sequence, $N_B=1000$ , $N_{OP}=10$ . . . . .	86
4.16	ROC Curve for GRLVQI TD Features, Authorized Verification	89
4.17	ROC Curve for GRLVQI TD Features, Rogue Detection . . .	91
4.18	ROC Curve for GRLVQI CD Features, Authorized Verification	93
4.19	ROC Curve for GRLVQI CD Features, Rogue Detection . . .	94

*List of Tables*

Table		Page
1.1	Previous Work vs. Current Contributions . . . . .	16
2.1	<i>Normal</i> vs. <i>Anomalous</i> Verification Outcomes . . . . .	30
3.1	DUT to PLC ID Mapping . . . . .	32

## *List of Abbreviations*

Abbreviation		Page
AFCEC	Air Force Civil Engineering Center . . . . .	5
AFCERT	Air Force Computer Emergency Response Team . . . . .	1
APP	Application Layer . . . . .	8
AT	Anti-Tamper . . . . .	2
AV	Anti Virus . . . . .	21
AWGN	Additive White Gaussian Noise . . . . .	46
CBAD	Correlation Based Anomaly Detection . . . . .	1
CD	Correlation Domain . . . . .	14
COTS	Commercial Off The Shelf . . . . .	2
CPU	Central Processing Unit . . . . .	32
DARPA	Defense Advanced Research Projects Agency . . . . .	7
DFT	Discrete Fourier Transform . . . . .	33
DLL	Data Link Layer . . . . .	21
DOD	Department of Defense . . . . .	1
DUT	Device Under Test . . . . .	11
EER	Equal Error Rate . . . . .	30
EM	Electro-Magnetic . . . . .	8
FADR	False Anomaly Detection Rate . . . . .	30
FADR	False Anomaly Detection Rate . . . . .	64
FNVR	False Normal Verification Rate . . . . .	65
FPGA	Field Programmable Gate Array . . . . .	2
GRLVQI	Generalized Relevance Learning Vector Quantized-Improved	14
HIDS	Host-based Intrusion Detection System . . . . .	18
HMI	Human Machine Interface . . . . .	18
IC	Integrated Circuit . . . . .	7

Abbreviation		Page
ICS	Industrial Control System . . . . .	1
ICs	Integrated Circuits . . . . .	3
ICS-CERT	ICS Cyber Emergency Response Team . . . . .	6
IDS	Intrusion Detection Systems . . . . .	5
IMEI	International Mobile Equipment Identity . . . . .	5
IRE	Intentional RF Emissions . . . . .	9
ISM	Industrial, Scientific, and Medical . . . . .	23
IT	Information Technology . . . . .	1
LAN	Local Area Network . . . . .	22
LFS	Learning From Signals . . . . .	14
LLPs	Ladder Logic Programs . . . . .	15
LPF	Low Pass Filter . . . . .	32
MAC	Media Access Control . . . . .	4
MCU	Micro Controller Unit . . . . .	32
MDA/ML	Multiple Discriminant Analysis/Maximum Likelihood . .	14
MOV	Move . . . . .	19
NWK	Network Layer . . . . .	8
OLE	Object Linking and Embedding . . . . .	20
OS	Operating System . . . . .	18
OS	Operating System . . . . .	6
OSI	Open Systems Interconnect . . . . .	4
PCs	Personal Computers . . . . .	6
PHY	Physical Layer . . . . .	8
PLCs	Programmable Logic Controllers . . . . .	2
PMF	Probability Mass Function . . . . .	73
PSD	Power Spectral Density . . . . .	32
RAM	Random Access Memory . . . . .	18

Abbreviation		Page
RF	Radio Frequency . . . . .	8
RF-DNA	Radio Frequency Distinct Native Attributes . . . . .	9
RFINT	Radio Frequency Intelligence . . . . .	14
RFSICS	RF Signal Intercept and Collection System . . . . .	25
ROC	Receiver Operating Characteristic . . . . .	17
ROI	Region Of Interest . . . . .	24
RTUs	Remote Terminal Units . . . . .	6
SCA	Side Channel Analysis . . . . .	8
SCADA	Supervisory Control And Data Acquisition . . . . .	1
SD	Spectral Domain . . . . .	14
SQR	Square Root . . . . .	19
TADR	True Anomaly Detection Rate . . . . .	30
TADR	True Anomaly Detection Rate . . . . .	64
TD	Time Domain . . . . .	14
TD	Time Domain . . . . .	15
URE	Unintentional RF Emissions . . . . .	9
USAF	United States Air Force . . . . .	1

### *Abstract*

The research goal involved developing improved methods for securing Programmable Logic Controller (PLC) devices against unauthorized entry and mitigating the risk of Supervisory Control and Data Acquisition (SCADA) attack by detecting malicious *software* and/or trojan *hardware*. A Correlation Based Anomaly Detection (CBAD) process was developed to enable 1) *software anomaly detection*—discriminating between various *operating conditions* to detect malfunctioning or malicious software, firmware, etc., and 2) *hardware component discrimination*—discriminating between various *hardware components* to detect malfunctioning or counterfeit, trojan, etc., components.

Defense against *software* exploitation was implemented by 1) adopting a previously demonstrated capability that provides human-like discrimination of hardware devices using information extracted from intentional Radio Frequency (RF) emissions, and 2) adapting an RF-based verification methodology to exploit information in unintentional PLC emissions to detect anomalous operation resulting from *software* and/or *hardware* discrepancies and enhance SCADA security. Operational status verification (normal versus anomalous) is demonstrated using experimentally collected emissions from ten Allen Bradley SLC-500 PLCs executing custom Ladder Logic Programs (LLPs) designed to support the research methodology.

Performance for verification-based *software* anomaly detection was evaluated using the CBAD process. The CBAD verification process is sequence agnostic and can be used with untransformed Time Domain (TD) or transformed inputs, including those derived from untransformed TD, Hilbert transform (HT), and RF Distinct Native Attribute (RF-DNA) features. Relative to performance using untransformed TD sequences or RF-DNA features, CBAD performance using HT sequences was superior with an arbitrary Receiver Operating Characteristic (ROC) curve Equal

Error Rate (EER) benchmark of  $EER_B \leq 10.0\%$  achieved for all PLC devices at a Signal-to-Noise Ratio (SNR) of  $SNR=0.0$  dB; this benchmark was not achieved for any PLCs using untransformed TD sequences or RF-DNA features.

Performance for verification-based *hardware* anomaly detection was evaluated using a Generalized Relevance Learning Vector Quantized-Improved (GRLVQI) process with two input sequences, including one derived from TD RF-DNA features ( $N_{Dim}=156$  dimensions) and one from Correlation Domain (CD) features ( $N_{Dim}=10$  dimensions). For this assessment, ten Allen Bradley PLCs were divided into *authorized/authentic* and *rogue/unknown* groups containing five devices each. The GRLVQI model was trained using sequences from all *authentic* devices and each device in the *unknown* group was presented for verification against each of the *authentic* devices (25 total anomaly assessments). The GRLVQI anomaly detection capability was assessed using each of the two input sequence types and resultant performance was comparable. At  $SNR=15.0$  dB an average  $EER \approx 1.3\%$  was achieved for TD sequences as compared to an average  $EER \approx 1.6\%$  for the CD sequences; both sequence types satisfied the  $EER_B \leq 10.0\%$  benchmark for all PLC devices. While the  $EER$  value for TD sequences is 0.3% lower than CD sequences, the TD sequence has nearly 16 times the number of elements as the CD sequence and a correspondingly greater amount of computational resources would be required in an operational implementation.



# RADIO FREQUENCY BASED PROGRAMMABLE LOGIC CONTROLLER ANOMALY DETECTION

## *1. Introduction*

This chapter introduces the research topic and outlines the motivation behind the development of the Correlation Based Anomaly Detection (CBAD) process described in later chapters. Section 1.1 provides a brief overview of the operational Supervisory Control And Data Acquisition (SCADA) and Industrial Control System (ICS) topology and vulnerabilities. It is further divided into two subsections: 1) Section 1.1.1 describing the *software*-based vulnerability picture for SCADA/ICS and 2) Section 1.1.2 describing the potential for *hardware*-based security concerns. Section 1.2 provides a brief description of existing research and technologies supporting the current research effort. Section 1.3 provides a summary of the existing research and technologies contributions.

### *1.1 Operational Motivation*

Modern digital computing technology has led to a proliferation of computers to nearly every aspect of daily operations for the United States Air Force (USAF) and Department of Defense (DOD) as a whole. The modern US military is critically dependent on computer hardware and digital communication systems to successfully carry out their mission from checking email to ordering needed maintenance parts. The advantages in efficiency through use of networked Information Technology (IT) resources brings with it the cost of increased vulnerability to malicious cyber attacks. The Air Force Computer Emergency Response Team (AFCERT) is the primary agency responsible for protecting USAF network assets from attack. The AFCERT

reported nearly 2 million weekly alerts indicating potential cyber attacks against USAF bases in the month of November, 2011 [99], highlighting the magnitude of cyber threats facing networked IT systems. In addition to the potential attacks, there have been over 150 verified incidents of “hackers” gaining access to information system assets affecting the USAF mission in 2011 [99]. The threat of attack and compromise of USAF information system assets directly affects nearly all aspects of the USAF mission.

A key aspect of information systems usage is the communication systems linking devices and networks. Data exchange occurs over computer networks (wired and wireless) as well as over civilian communication networks (i.e., cellular/satellite phone networks). The analysis and storage of potentially sensitive data is reliant, to a large extent, on Commercial Off The Shelf (COTS) products either slightly modified for military use or not altered at all. In order to ensure proper control and verification of the data relevant to the military mission, it is essential that the devices used to manage the data are trusted. Various vulnerabilities exist in the communication systems and data processing hardware currently used in military applications. Although methods exist to protect hardware and communication signals from exploitation, such as Anti-Tamper (AT) initiatives for hardware and data encryption for communication systems, these methods are not sufficient to guarantee the authenticity of computing platforms, programs, or communication nodes.

Another, less publicized, area of concern involves *hardware*-based vulnerabilities. The focus on cheaper semiconductor devices, such as those at the core of SCADA Programmable Logic Controllers (PLCs), has led to a heavy reliance on overseas manufacturing that results in a greater risk of potentially damaging trojan or counterfeit devices being deliberately used on PLC devices in critical applications [17,82]. For example, the DOD implemented a ban on the use of thumb drives following concerns regarding virus transmission via the flash drive medium [8]. Military Field Programmable Gate Array (FPGA) systems are prone to exploitation

given their reconfigurable nature. Even Integrated Circuits (ICs) fabricated for US military use are vulnerable given the majority of manufacturing facilities are located overseas. Although research has been focused towards combating the threat of hardware and communication vulnerabilities [53, 69, 70, 90], the verification of a hardware platform, program, or communication node is critical to protecting and validating the data used in carrying out every aspect of the USAF military mission.

Information Technology systems have also yielded unprecedented levels of automated, precise control of ICS operations for functions from waste water treatment to nuclear power generation. ICS facilities maintain critical infrastructure capabilities in the civilian and Government sectors. US Government policy states “Private business, government, and the national security apparatus increasingly depend on an interdependent network of critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors” [98]. Current ICS architectures are predominantly based on networked digital computers that enable reliable monitoring and control of critical functions within regionally localized and globally distributed operations [84]. One key element of the ICS operation are SCADA systems. These provide centralized control and monitoring via PLC devices, which are the gateway through which recent cyber attacks have been orchestrated against high-profile ICS targets [95, 105]. The majority of publicized attacks target *software*-based vulnerabilities to inflict damage [12, 13, 33, 44, 60, 93, 94]. While the software vulnerabilities may lie within a PLC or other SCADA component, PLCs represent the last component to operationally implement *kinetic* effects caused by a cyber attack.

With such reliance on the critical functions performed by ICS assets and facilities, the SCADA and PLC systems employed must be secured from cyber attack similar to how major IT systems are currently protected and secured. Unfortunately, there exists a gap between the security options for ICS assets and IT systems. PLCs tend to be specific purpose machines and often are out-dated by IT standards. There

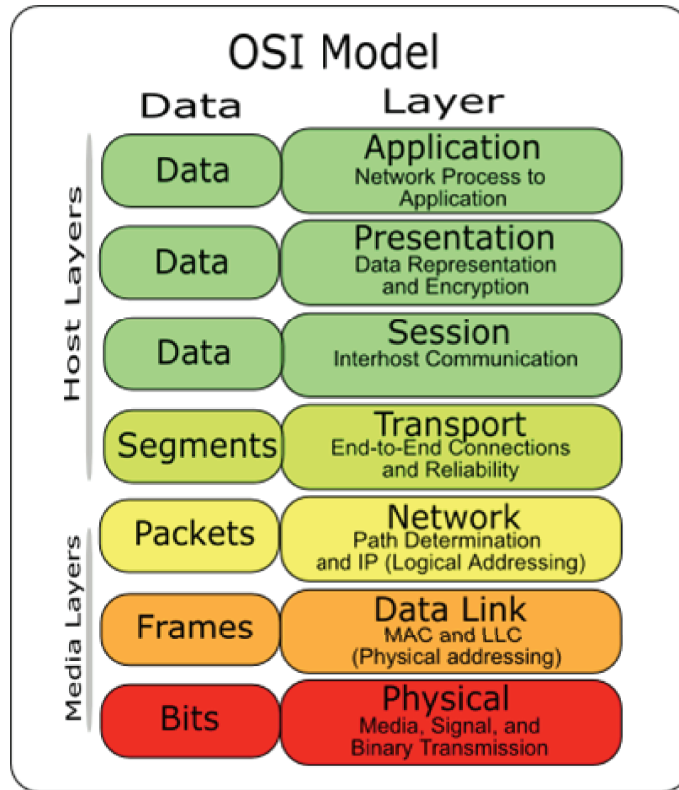


Figure 1.1: OSI 7-layer network model [7].

is not an availability of applications available for the PLCs aside from the applications needed to perform their specific tasks. There needs to be a method of detecting altered or anomalous activity on SCADA and PLC hardware to thwart adversarial attacks.

Consider the Open Systems Interconnect (OSI) model describing the different levels of a system [106] shown in Fig. 1.1. The current focus on detection of unauthorized or anomalous activity on information systems is through analysis of the data within the Application (Layer 1) or Network (Layer 5) layers of the model. In communication systems such as cellular phone systems and wireless networking, data access and trust relationships are commonly verified via verification methods operating in the Data Link Layer (Layer 2) of the OSI model. These verification credentials include Media Access Control (MAC) addresses for wireless network access

and International Mobile Equipment Identity (IMEI) numbers for cellular networks. These verification methods are far from foolproof. There exist tools and methods allowing an individual to modify the verification credentials, allowing adversaries to bypass the Data Link Layer control measures all together [61, 73, 104]. IT networks employ firewalls and network Intrusion Detection Systems (IDS) components to detect and block cyber attacks. IT systems employ virus detection and host-based IDS programs to perform similar functions at the individual computer level. SCADA and PLC systems are special purpose machines and do not have the general purpose capabilities of most desktop or server computers in the IT realm. Additionally, it is not uncommon to see ICS components, to include PLCs, installed and in operation for decades. These PLCs do not have the functionality to run the virus detection or IDS programs. This exposes the system to threats that have the potential to enact substantial physical losses as in the case of StuxNet or the Springfield attacks.

The following sections address the research motivation in light of two primary attack vectors used to exploit PLC vulnerabilities, including 1) Section 1.1.1 which addresses *software*-based vulnerabilities, and 2) Section 1.1.2 which addresses *hardware*-based vulnerabilities.

*1.1.1 Software-Based Vulnerabilities.* Network and computer security experts at McAfee predict 2013 will bring a shift in the cyber warfare picture that includes increased activity in nation state’s becoming victims and targets of cyber attacks [63]; McAfee suggests improving SCADA system defense by removing them from the production network and placing them on a dedicated stand-alone network. The motivation for removing SCADA systems from the production network is due in part to the number of potential high-value critical infrastructure ICS targets (civilian and military) using SCADA control via an unsecure network. The Air Force Civil Engineering Center (AFCEC) states that ICS assets in the USAF and in industry are “at best insufficiently protected from cyber threats” [100]. In acknowledgement of the criticality of US ICS infrastructure, the US Government has prioritized the

defense of these vulnerable assets through a Presidential Directive in 2003 [5] and more recently through an Executive Order in 2013 [66]. Despite the focus on protecting ICS assets from malicious activity, they still remain vulnerable. Over 20 vulnerability alerts and advisories have been issued from the ICS Cyber Emergency Response Team (ICS-CERT) in January of 2013 alone [46]. Therefore, protecting vital ICS assets from the risk of cyber attack is essential and is a key component used to mitigate the potential catastrophic consequences if an attack occurs.

SCADA systems typically monitor and control higher-level systems through field-based devices called Remote Terminal Units (RTUs) or PLCs that physically implement desired functionality. A PLC is a special purpose computer that performs low-level ICS functions, such as collecting sensor data and operating physical valves or switches [84]. While the PLC Operating System (OS) and communication protocols are often proprietary, most current PLCs have the ability to operate on a standard network. It is through these networks that malicious programs are loaded onto vulnerable PLCs. A majority of electronic devices, including Personal Computers (PCs) and network components, are protected to some degree from cyber attacks through a variety of intrusion detection and/or anti virus programs. This is in sharp contrast to PLC implementations, which have very limited protection options due to proprietary design, limited processing power, and limited memory that precludes direct use of standard PC and network anti virus programs [82]. Additionally, many PLCs remain in service for decades due to the prohibitive cost of re-engineering SCADA systems. Thus, PLCs become obsolete and unsupportable relative to IT standards and capabilities that continually evolve to satisfy consumer demands preventing the implementation of typical “bit-level” IT protective measures in PLC devices. ICS facilities remain vulnerable to cyber attack as evidenced by recently successful Stuxnet malware-based attack [105]. More recently, sophisticated programs including ICS specific malware, such as Duqu and Flame, demonstrate a continued need for SCADA and ICS defensive research. These malware programs

contain computer code that targets SCADA and ICS functions through vulnerable components [12, 13, 93, 105]. Consequently, there is a vital need to implement a process to detect malicious code installed on PLCs *before* the code can execute and cause irreversible, catastrophic effects.

*1.1.2 Hardware-Based Vulnerabilities.* In addition to the high-profile *software*-based attacks, concern also exists regarding *hardware*-based compromise orchestrated through trojan or counterfeit semiconductor or Integrated Circuit (IC) devices. Semiconductor devices are prevalent and form the core of all computer systems in use today including those related to SCADA systems and ICS infrastructure. Systems relying on secure semiconductor and IC devices are integrated within ICS facilities and in use throughout DOD to process, store, and protect sensitive information remain vulnerable to tampering by adversaries. Not all forms of attacks are malicious in nature. Counterfeit, used, or sub-standard quality devices can fail in critical applications, causing similar damage compared to a malicious attack. The general term *component substitution* can be used to refer to the substitution of a genuine, trusted component with a counterfeit, substandard, or trojan component. This substitution can be made during manufacture, assembly, transport or even after operational deployment. Unfortunately, most organizations in the DOD do not have the means to defend against counterfeit or trojan component substitution [4]. Estimates of the losses due to counterfeit semiconductor devices are staggering. The losses are estimated at approximately \$200B USD with about 10.0% of electronic parts in use being counterfeit substitutions [65]. The intent of substitution varies from malicious exploitation of DOD systems to increasing company profits by using cheaper components. To combat the proliferation of potentially harmful IC devices in DOD applications, the Defense Advanced Research Projects Agency (DARPA) is attempting to combat potential trojans in DOD ICs manufactured in foreign countries as part of the Trusted IC program [17]. This program is technologically in its

infancy. Additional work is required to verify IC authenticity using *non-destructive*, *non-disruptive* techniques that enable device verification during operation.

## 1.2 Technical Motivation

Traditional bit-level intrusion detection and anti virus programs monitor activity and assess system status using information in higher layers of the OSI model [106]. One possible solution is to change the focus of detection from the Application (APP) and Network (NWK) layers to the Physical (PHY) layer. Detection of anomalous activity in the Physical layer is dependent on the analysis of physical attributes of the system operation, such as power consumption, heat, or Radio Frequency (RF) radiation from a specific ICS device. Research efforts have proposed one such method of detecting the anomalous behavior due to the presence of trojan hardware contained in an IC package using Side Channel Analysis (SCA) methods to capture signals from the outputs of the ICs [2]. This method could potentially be extended to identify and categorize the operation of a known device. Although this method provided positive results, it requires exercising all of the expected operations in order to effectively identify the operations. Additionally, the IC would need to be isolated to minimize effects of other components on the same circuit board. Other research efforts have used a method of detecting anomalous operations through power analysis [28, 29]. Using a non-contact Electro-Magnetic (EM)-based instantaneous current probe, the operating current is captured and used to estimate the power usage of the IC. The probe must be placed at the power trace for the IC in question, which could change for different implementations. Variations in power usage based on the variations in IC manufacture, device temperature, and other components drawing power from the same power trace can complicate the measure of current draw for the targeted IC. What is needed is a validation method that does not require removal of the IC and can non-destructively analyze the operations while limiting interference from other system components. Detection and classification of devices and device operations



based on RF attributes and qualities have been successfully demonstrated in a large body of research [9, 11, 14–16, 18, 19, 21, 23–25, 27, 34, 39, 42, 49, 77, 79, 81, 103]. The use of attributes from the RF emissions provides a means of detecting anomalous activity on a wide range of systems without the limitations imposed by the lack of PLC IDS and Anti Virus (AV) program capabilities. One proposed method of verifying the identity of either a communication node or a hardware platform is through collection, analysis, and classification of the RF energy emitted by the device. RF Fingerprinting can be used to generate unique IDs for a given device based on its physical attributes. A key advantage to RF Fingerprints is the relative difficulty in spoofing or altering the RF Fingerprint for a device as compared to spoofing or altering the network or hardware credentials.

At the core of PLCs (and most information systems technologies) are semi-conductor IC devices. There are potential variabilities in materials, processes, and environmental variables involved the semi-conductor manufacturing process. These variances result in physical differences in IC devices even if the devices are designed to be equivalent. Device testing limits the variance in devices sold to consumers by testing to ensure the functional characteristics of the devices are within a defined tolerance. Functional testing is a well researched and developed field [1, 54, 55]. Functional testing is generally limited to verifying the device outputs are correct for the expected clock timing and voltage levels variance. Within the tolerance are variances in performance that can be detected and quantified using specific test equipment. The idea of Radio Frequency Distinct Native Attributes (RF-DNA) is based on capturing, analyzing, and quantifying variance in RF emissions related to variances in manufactured semi-conductor devices. The term RF “fingerprint” is used to describe the RF-DNA values associated with a specific device.

RF fingerprints can be derived from two broad categories of RF emissions, including Intentional RF Emissions (IRE) and Unintentional RF Emissions (URE). Substantial research has been conducted using RF energy attributes to produce

RF fingerprints for device verification [6, 11, 35, 37, 38, 57, 58, 75, 80, 91, 92, 97]. IRE describes RF energy that is intentionally broadcast as part of a device’s function. Examples of devices that broadcast IRE include wireless radios, IEEE 802.15 Bluetooth devices, cellular phones, and IEEE 802.11 WiFi networking devices. While wireless communication devices make use of IRE to perform their primary function, digital hardware devices also have URE related to the logic switching in the device. URE describes RF energy that is unintentionally broadcast during device operation. The URE is not beneficial to device operation and is considered a detriment as it can interfere with normal operations. The operation of clock signals for IC circuits is one contributor to the broadcast of URE from IC-based devices.

RF fingerprints have been used to identify and verify devices. The identification of a device is a means of comparing a single RF fingerprint to a set of established fingerprints and “classifying” the device as one of the previously analyzed devices based on a comparison of the RF fingerprints. This is a one-to-many comparison problem, meaning a single fingerprint is compared to multiple classified fingerprints in order to properly identify the device. The verification of a device is a means of comparing a single RF fingerprint to a single previously captured and analyzed fingerprint and determining to what extent the two fingerprints are similar. This is a one-to-one comparison problem meaning a single fingerprint is compared to a single classified fingerprint in order to verify the device.

The following sections provide a brief overview of previous efforts in the field of RF fingerprints for the purpose of classification and verification for both IRE and URE RF signal responses.

*1.2.1 Emission Collection.* The use of Physical layer RF characteristics to classify and verify wireless devices or operations has been well researched [6, 25, 36, 38, 58, 59, 68, 92, 96, 97, 102, 103]. Regardless of emission type (IRE or URE) being

considered, RF fingerprinting and device classification generally involves a basic 5-step process that includes [79, 91]:

1. Signal Collection
2. Burst Detection
3. Feature Extraction
4. RF Fingerprint Generation
5. Device Classification

Each step of the process is tailored to the wireless technology and device characteristics of the Device Under Test (DUT) as specified in the device design specifications. The generic classification process provides a starting point for using RF emissions to discriminate between devices or operations.

The subject of using Physical layer RF characteristics to classify and verify URE devices has not been as well researched as the IRE case. There has been research and work focused on leveraging differences in output signals from ICs to verify authenticity of the physical design, but they do not consider URE RF signals from the device itself [2, 53]. Recent research efforts provided some of the initial work in the field of capturing the RF signals from the IC DUTs for the purpose of classification and verification [10, 11] differing from the IRE process primarily in the collection portion of the process.

The targeted RF signals for URE device exploitation differ from IRE device exploitation in that there is no specified design for the signal as there are for wireless broadcast standards. Additionally, the URE signal is not intentionally broadcast and so the average signal power is significantly lower than that of an IRE signal. The signal is collected using an RF probe instead of an antenna. The collection specifics and configuration (such as bandwidth and target frequency) are largely determined by the DUT clock frequency and empirically developed based on observation of captured RF signals.

*1.2.2 Fingerprint Generation.* Once the signal for an IRE or URE DUT has been collected, sampled, filtered, and stored, the fingerprint generation step of the process is performed. The specific fingerprint generation process considered is that used for AFIT’s RF-DNA work [10, 58, 79, 103]. The fingerprint generation is largely device agnostic in that regardless of whether the signal is based on collection against an IRE or URE DUT, the high-level methods used to generate the fingerprint are identical. Changes to the process are limited to configuration of the tools used to generate the fingerprints.

The fingerprints are based on statistical attributes of signal characteristics such as amplitude, frequency, and/or phase. The statistical attributes include standard deviation, variance, skewness, and kurtosis. Prior to the calculation of the signal characteristics and statistical attributes, a variety of transforms can be performed on the collected, sampled discrete signal dependent on the DUT signal qualities.

*1.2.3 Device Classification.* A majority of existing RF fingerprints research involves the classification of the DUT based on previously examined data sets. The process involves analyzing RF fingerprints for known devices. The fingerprints from the known devices are used to train software known as a classifier. In essence, the training establishes fingerprint characteristics aligning an unknown DUT fingerprint to a previously established device class based on the results of the training process.

Classification of devices is a one-to-many comparison that typically leads to a DUT being classified as one of the available known devices. The research goal is to verify a PLC is operating “normally”. One of the difficulties in classification is to define linear (when possible) or non-linear boundaries separating class fingerprints with a certain degree of accuracy. The problem of verifying a PLC is operating normally can be tackled as a two-class problem: normal operating condition class or anomalous operating condition class. It is easier to define a linear boundary for a two-class problem than a multi-class problem. However, a more direct and

simpler solution may be the use of verification instead of classification for the goal of monitoring PLCs for anomalous activity.

*1.2.4 Device ID Verification.* One goal for capturing RF emissions and extracting RF fingerprints is to verify a device’s bit-level ID; this is related to device verification which is commonly used for granting network access. Verification is a one-to-one comparison of an unknown DUT fingerprint to a known device fingerprint with a goal of determining if the unknown DUT is the known device. This process can be compared to using a photo identification card to verify an individual’s identity.

Using RF fingerprints for DUT ID verification is not as well researched as using RF fingerprints for device classification. Previous research efforts were able to demonstrate the use RF fingerprints to verify PIC microcontroller semi-conductor devices [11] and wireless devices [76]. The process of comparing RF fingerprints to verify a device’s ID parallels the procedures used for biometric human ID verification. Biometric classification and verification provides a well-established framework that is well-suited to the challenge of verifying PLC operations [48].

Following the general biometric verification process using RF fingerprints, previous researchers were able to accurately verify specific PIC microcontroller devices with better than 99.5% accuracy [11]. This success highlights the potential applicability for using verification-based methods to assess PLC device operational state (normal or anomalous).

*1.2.5 Correlation and Matched Filtering.* Previous RF fingerprinting processes relied heavily on classification methods. While effective, the implementation of these classification methods can become computationally expensive for a large number of classes and/or RF fingerprint characteristics. Yet, work continues and there exists multiple efforts aimed at quantifying and reducing the computational complexity of classification processes [3, 43]. The complexity of classification pro-

cesses is of concern when implementing the processes on information systems with limited processing power such as mobile platforms or systems with power constraints.

One potential alternative to approaching the problem involves using relatively simple correlation-based methods for classification. Correlation is a key function that is commonly used in optimal implementations of matched filtering for estimating digital communication symbols [72, 85]. Additionally, the correlation function has found use in image processing and other fields requiring identification of signals where signal noise may be an issue [20]. Correlation is conceptually a straight forward function with a well-defined complexity. Correlation provides an attractive alternative for classification given its simplicity and predictable computational complexity.

### 1.3 Research Contributions

The research goal involved expanding the knowledge base of Physical layer methods being developed to reliably detect anomalous and/or malicious activity within ICS components. Specifically, the research objectives included developing a general verification-based anomaly detection approach to support both 1) *software anomaly detection*-discriminating between various *operating conditions* to detect malfunctioning or malicious software, firmware, etc., and 2) *hardware component discrimination*-discriminating between various *hardware components* to detect malfunctioning or counterfeit, trojan, etc. ICs. As summarized in Table 1.1, AFIT research contributions in the Radio Frequency Intelligence (RFINT) field have been made in several technical areas. Previously undefined acronyms that are used in the table include: Time Domain (TD), Spectral Domain (SD), Correlation Domain (CD), Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML), Generalized Relevance Learning Vector Quantized-Improved (GRLVQI), and Learning From Signals (LFS).

## 1.4 Document Organization

The remaining chapters are organized as follows. Chapter 2 provides background information regarding SCADA and ICS systems, PLCs, Ladder Logic Programs (LLPs), network/PLC vulnerabilities, spurious RF signal collection, post-collection processing, the correlation operation, the Hilbert transform, and device verification. Chapter 3 provides details on the methodology used for this research effort including signal collection and processing, the CBAD process, the RF-DNA process, the specific devices and LLPs used for this research, and the verification metrics presented to measure performance. Chapter 4 presents the results of the methodologies from Chapter 3 including *verification* performance for CBAD and RF-DNA processes for (TD) and Hilbert transformed waveforms. Chapter 5 provides a summary of the research results and potential future research efforts.

Table 1.1: Relational mapping between RFINT *Technical Areas* in *Previous* related work and *Current* AFIT research contributions. The  $\times$  symbol denotes specific areas addressed.

Technical Area	Previous Work		Current Research	
	Addressed	Ref #	Addressed	Ref #
TD Features	$\times$	[57, 58, 76, 77] [91, 92, 102, 103]	$\times$	[86–89]
SD Features	$\times$	[10, 11, 81, 103]		
CD Features	$\times$	[91, 92]	$\times$	[86–89]

Emission Type				
Intentional (IRE)	$\times$	[57, 58, 76, 81] [91, 92, 102, 103] [21, 39, 40, 42]		
Unintentional (URE)	$\times$	[9–11]	$\times$	[86–89]
Burst	$\times$	[57, 58, 76, 81] [91, 92, 102, 103] [21, 39, 40, 42]		
Continuous	$\times$	[9–11]	$\times$	[86–89]
High SNR	$\times$	[57, 58, 76, 81] [91, 92, 102, 103] [21, 39, 40, 42]		
Low SNR	$\times$	[9–11]	$\times$	[86–89]

Classification/Verification Processes				
MDA/ML	$\times$	[57, 58, 77, 81] [91, 92, 102, 103] [9–11, 21]		
GRLVQI	$\times$	[57, 58, 77, 81]	$\times$	
LFS	$\times$	[39–42]		

Dimensional Reduction Analysis (DRA)				
MDA/ML	$\times$	[39, 57, 58, 77, 81]		
GRLVQI	$\times$	[56, 77, 81]	$\times$	
LFS	$\times$	[39–42]		

Verification				
Electronic Components	$\times$	[9–11]	$\times$	[89]
Authorized Wireless Devices	$\times$	[21, 77, 81]		
Rogue Wireless Devices	$\times$	[21, 77, 81]		
Device Operations			$\times$	[86–88]



## 2. Background

This chapter provides background information on the topics associated with the research in support of developing a single verification-based anomaly detection approach supporting: 1) *software anomaly detection*-discriminating between various *operating conditions* to detect malfunctioning or malicious software, firmware, etc., and 2) *hardware component discrimination*-discriminating between various *hardware components* to detect malfunctioning or counterfeit, trojan, etc. Integrated Circuits (ICs). For the purpose of the research, *verification* is the validation of a claimed identity for either an *operating condition* or *hardware component*.

Section 2.1 provides background on Supervisory Control and Data Acquisition (SCADA) and Industrial Control System (ICS) and outlines the relationship between Programmable Logic Control (PLC) devices and the Ladder Logic Programs (LLPs) used to control them. Section 2.2 provides background related to SCADA and ICS vulnerabilities. Section 2.3 outlines the general emission collection and post-collection processing used for Time Domain (TD) signals. Section 2.4 provides a description of the two primary signal processing methods implemented in the research, including correlation in Sect. 2.4.1 and the Hilbert transform in Sect. 2.4.2. The chapter concludes with Sect. 2.5 which provides details on the verification-based anomaly detection process and Receiver Operating Characteristic (ROC) curve metrics used for quantifying verification process performance.

### 2.1 SCADA and ICS Applications

As used in this document, the term SCADA refers to the entire collection of hardware, software, and network elements that directly support monitoring and control of ICS functions and facilities. ICS functions and facilities include, but are not limited to, manufacturing, power generation, waste-water treatment, and transportation control. SCADA systems are constructed in a hierarchical manner

with *supervisory* systems providing monitoring and top-down control of field devices, such as PLCs and Remote Terminal Units (RTUs). Field devices are used to collect telemetry, which may be used to control field device operations or transmitted to a Human Machine Interface (HMI) for observation and recording. PLC functionality is controlled through LLPs which are computer programs written in a PLC specific programming environment. While HMIs play an important part in overall SCADA functionality and operation, PLCs and their controlling LLPs were the focus of this research effort.

*2.1.1 Programmable Logic Controller (PLC).* PLC devices are used to implement low-level functions within a SCADA system. At the simplest level, PLCs collect various sensor inputs, run LLP operations using the input values, and assign outputs based on the program results. A PLC device is typically comprised of a microprocessor/microcontroller, associated Random Access Memory (RAM) and firmware for executing the LLPs, input connections for collecting sensor data, output connections for controlling physical electro-mechanical devices (relays, valves, motors, etc.), and communication connections for interfacing with other devices or for direct human interaction.

Relative to current main-stream Information Technology (IT) products, the microprocessor, RAM, and firmware used in a majority of currently deployed PLCs are outdated and lagging in performance. Thus, they are not capable of executing programs such Host-based Intrusion Detection System (HIDS) software that is commonly used in IT applications to provide internal defense against malicious or unauthorized programs. PLCs are installed within a variety of physical environments that prioritize robustness over computational capability and require relatively simple hardware with demonstrated reliability and resilience to harsh environmental effects. The unique hardware of PLCs necessitates specially designed Operating System (OS) software for interfacing between the hardware and the user-implemented LLPs. The defensive security programs and processes that are commonly implemented in tradi-

tional IT systems are not applicable to PLCs due to the hardware differences between traditional IT systems and PLCs [82]. Thus, SCADA field devices do not benefit from a large body of research and technologies aimed at improving IT security.

*2.1.2 Ladder Logic Program (LLP).* LLP implementation allows users to control the processing of PLC inputs and outputs. The LLP language is unique to the PLC/SCADA environment and is largely based on the physical design of relays that were used prior to introducing PLCs to control ICS functionality. Figure 2.1 shows an example of an LLP as programmed in the Allen Bradley RSLogix<sup>®</sup> programming environment consisting of Move (MOV) and Square Root (SQR) LLP operations. As presented, these programs are structured as inputs on the left and operations/outputs on the right. Apart from branching capability that is inherently supported in PLCs, the LLPs fundamentally operate in sequential order. For the PLC devices considered under this research, the execution of experimental LLPs was strictly sequential with no recursive calls or nested function included; this ensured that PLC operation was deterministic and that resultant research conclusions were based on experimentally repeatable execution.

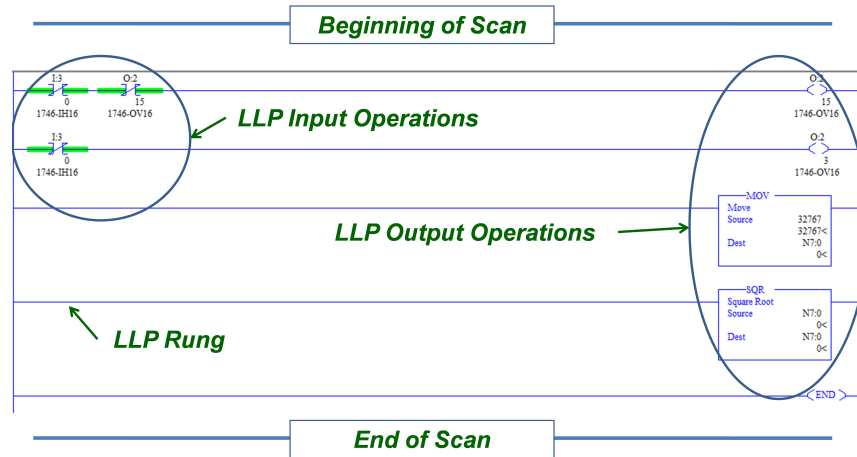


Figure 2.1: Representative LLP constructed in the Allen Bradley RSLogix<sup>®</sup> programming environment consisting of a single MOV and SQR operation. Program rungs in the ladder are executed sequentially from left-to-right, top-to-bottom.

LLP programs are inherently repetitive, with each repeated execution cycle beginning at the top LLP *rung* and ending at the last program rung. Each execution of the LLP is called a *scan*. For each LLP scan, the inputs are all processed and read into memory first. The outputs are then logically computed and stored in internal registers based on the logic of the LLP. The final step of the LLP scan is to assign all computed outputs to the actual, physical outputs of the device. The PLC then begins the next scan at the top rung of the LLP. While branches may exist in the LLP, recursive calls or *do-while* loops are not permitted as the scan is fundamentally a linear left-to-right, top-to-bottom, progression through the LLP.

*2.1.3 Human Machine Interface (HMI).* HMIs provide a means for users to observe, monitor, and control ICS functions. HMIs are fundamentally software packages installed and executed on standard Personal Computers (PCs). HMI software is programmed to interact with PLCs and other field devices through IT network media using SCADA communication protocols such as the Object Linking and Embedding (OLE) process control. While PLCs represent one means through which malicious events can be physically enacted upon the system, the HMIs represent an easy means for malicious software to be loaded onto victim PLCs [12, 13, 93, 94]. For example, attacks similar to Stuxnet obfuscate the operator’s view of the victim PLC status by using altered LLPs that replace legitimate LLPs stored on the PLC [105]. Despite the vulnerability, HMIs remain essential and provide valuable insight into ICS facility functions by assimilating data from various Remote Terminal Units (RTUs) and PLCs and presenting it in a customizable format to ICS facility operators.

While HMIs pose a potential vulnerability, the fact that a majority of the HMIs are built from standard IT components significantly mitigates the threat. Widely available IT security programs, tools, and methods are applicable to the majority of HMI systems. Additionally, the communication networks consist of Commercial Off The Shelf (COTS) IT devices and protocols. There may be proprietary protocols operating between field devices, but these protocols typically operate over standard

IT infrastructure and can be monitored for potentially destructive activity similar to how standard protocols are monitored [64].

## *2.2 SCADA and ICS Vulnerabilities*

SCADA and ICS systems remain vulnerable to a variety of attacks and methods of compromise. The ICS Cyber Emergency Response Team (ICS-CERT) maintains a list of hundreds of vulnerabilities specifically affecting SCADA and ICS components and systems [45]. The vulnerabilities affect multiple devices within the SCADA hierarchy, including both PLCs and HMIs. HMI hardware implementations are largely based on traditional IT systems and benefit from the substantial research in IT network defense. HIDS programs offer a means to detect unauthorized programs on HMI systems and Anti Virus (AV) software provides another avenue for detecting and removing malicious code on traditional IT systems. As stated in Sect. 2.1.1, PLCs are largely vulnerable in this respect due to a lack of defensive software or methods inherent in their design. Malicious threats such as Stuxnet exploit this vulnerability to inject malicious unknown code into SCADA systems.

The PLC field devices pose a particularly alarming threat due to the lack of general purpose processing capability, proprietary nature of the devices, and the long tech-refresh cycles for installed devices. The LLPs introduced in Sect. 2.1.2 are focused on providing industrial monitoring and control functions and are not general purpose enough to effectively implement AV or IDS functions, leaving the PLC devices vulnerable.

Extensive research effort has been applied to secure traditional Information Technology (IT) systems and networks by controlling access and detecting malicious programs, or malware, in the higher layers of the network Open Systems Interconnect (OSI) model, i.e., the Data Link Layer (DLL) through the Application (APP) layer. Bit-level credentials, such as Media Access Control (MAC) addresses and International Mobile Equipment Identity (IMEI) numbers control, control network

access while AV and Intrusion Detection System (IDS) software protects IT systems from malware. Had the IT protection methods been available for PLCs at the time of attack, the adverse effects of Stuxnet [105] and Duqu [93] malware-based attacks may have been mitigated. The programs offering defense of commodity IT assets are generally not implementable on the majority of PLCs and other ICS components within SCADA systems; therefore, the goal is to find alternative defense mechanisms that can be implemented on PLCs and other ICS components that are currently vulnerable. One specific alternative has emerged that exploits Radio Frequency (RF) emissions to achieve human-like discrimination of hardware devices using PHY Layer information extracted from either *unintentional* or *intentional* RF emissions to augment bit-level network access control measures [11, 18, 25, 58, 79, 102].

### 2.3 RF Emission Collection

Signal collection is the process of capturing and storing the Device Under Test (DUT) signal. The signal collection can either be accomplished using an antenna for Intentional RF Emissions (IRE) exploitation or using an EM probe for Unintentional Radiated Emanation (URE) exploitation. In either case, the equipment and process must be tailored to the specific target and signal attributes desired. Previous RF-based research can be broadly categorized based on the type of emission(s) exploited. IRE energy comes from devices that *intentionally* broadcast or emit RF radiation in support of their primary “by design” function (e.g., cellular phones, pagers, wireless Local Area Network (LAN) adapters, etc. URE energy comes from devices that emit RF radiation as an *unintended* by-product or “side-effect” of their primary function; the majority of electrical Integrated Circuit (IC) components emit some amount of RF radiation during the course of normal operation.

IRE RF signals are broadcast at a carrier frequency specified by the specific design of the DUT broadcast technology. The carrier frequency is typically much higher than the frequency bandwidth of the DUT RF signal [85]. For example IEEE

802.15 Bluetooth communications, use the Industrial, Scientific, and Medical (ISM) RF band residing at a carrier frequency of  $f_C=2.4$  GHz, but the Bluetooth signal has a bandwidth of less than 500 MHz [47]). Signals sampled at the carrier frequency of  $f_C=2.4$  GHz would require substantial storage and bandwidth if sampled and stored at the Nyquist-Shannon criteria (sample frequency  $f_S \geq 2f_C$ ). Therefore, the signal is down-converted after initial capture to a lower frequency with lower storage requirements. This down-converted signal meets the Nyquist-Shannon criteria for the DUT RF signal adjusted to account for the carrier frequency.

For a collection against an IRE device, critical collection aspects include the antenna used to receive the signal and the receiver used to format and store the signal. Additionally, even with the same receiver, different signal technologies will require different collection settings such as center frequency, filter bandwidth, sampling rate, and signal gain. Storage and processing also require specific collection methods and settings. Environmental conditions also have an effect on the collection as temperature and RF interference both impact captured signal. Previous RF Fingerprinting efforts have taken steps to limit the environmental impact such as operating the collection receiver from within a climate controlled automobile [25] or performing the collections indoors [79]. Although an uncontrolled environment presents a challenge to collecting IRE signals, other researchers have had success in collection and fingerprinting in an operational test environment with limited or no control over potential interference or environmental effects [34, 102].

Collecting against URE parallels the collection against IRE devices, but requires different equipment and collection methods. There exists invasive and non-invasive techniques for RF capture from URE devices. Given the goal of RF fingerprinting, to accurately identify hardware or operations, most collections will require non-invasive collections. One method of non-invasively collecting a URE signal is by using an Electro Magnetic (EM) probe. Previous related research has exploited differences in electrical responses collected directly from various IC connecting pins

(power, timing, control, data, etc.) to verify physical design authenticity [2, 28]; physical contact assessment. These methods are unlike RF-based method adopted for this research whereby RF emissions are collected from operating ICs using a near-field probe placed in close proximity to the DUT [11, 52]; non-contact electromagnetic assessment.

The RF signal must still be sampled for the purpose of storing and analyzing. The signal characteristics are based on physical attributes of the DUT and not specified design, so the sampling rate is determined empirically by analyzing the signals collected from the DUT. As in the case of IRE collection, the sampled signal may be filtered by a Low Pass Filter (LPF) to increase the overall Signal-to-Noise Ratio (SNR). Because the URE broadcast is not based on a specific design, the values for the LPF are determined empirically based on the spectral characteristics of the DUT URE RF signals. Another difference between the URE and IRE collection process is the burst detection. The IRE signals considered are transmitted in bursts containing well documented regions. The URE signals construction is an artifact of the operational design and it does not follow any structured arrangement or organization. Therefore, much of the time range for the Region Of Interest (ROI) is determined empirically based on visual examination of collected signals.

As mentioned previously, the equipment used to collect RF signals in support of fingerprinting differ for specific collections. For example, the signal specific equipment would include tuned antennas for IRE or EM detection equipment such as a near field probe for URE collection. In addition to the equipment required to capture the RF signals on the physical layer, the signal data must be collected and stored for future processing.

The URE fingerprinting research field has less subject matter and research than the IRE research field. There have been no less than four AFIT research efforts in the field of IRE related to GSM, 802.11x, and 802.16 technologies. To the best of the author's knowledge there has only been one dedicated AFIT research



effort related to the field of URE fingerprinting. Therefore, while the RF Signal Intercept and Collection System (RFSICS) collection metrics referenced above span multiple research efforts and wireless technologies, the AFIT-specific metrics for URE Fingerprinting are obtained from the previous PIC microcontroller work [10]. For the collection of URE data, recent AFIT efforts have used a *Riscure* near-field probe in place of an antenna for IRE and capture/store the data using a *LeCroy* 104-Xi-A Oscilloscope. A filter was implemented between the near-field probe and the oscilloscope to filter signals greater than 1 GHz. Since URE devices do not intentionally broadcast an RF signal at an advertised frequency, as is the case with IRE devices, the data collection settings are based on clock cycles and empirical results. The target PIC devices operate at a clock rate of 29.48 MHz. However, the collection was performed at a sampling rate of 2.5 Gsps (satisfying Nyquist sampling criteria for signals less than 1.25 GHz) in order to allow post-collection simulations using the extra data [10].

*2.3.1 Near-Field RF Probe.* RF energy can be collected using a typical far-field antenna (common for IRE collections) or in the near-field using a specific variant called an RF probe (common for URE collections). The near-field RF probes used for this research were manufactured by Riscure and composed of a tuned, calibrated conductive coil and low-noise amplifier. RF probe performance is primarily characterized by its *bandwidth* and *spatial resolution*, where *bandwidth* represents the frequency range over which the probe is sufficiently sensitive to collect RF emissions of interest and *spatial resolution* is the physical area extent over which the probe maintains this sensitivity.

*2.3.2 Digital Sampling.* A continuous, real-world signal contains an infinite number of values between any two points in time and would require an infinite amount of storage and processing power to analyze. Therefore, the continuous RF signal broadcast from the DUT must be sampled for storage and analysis. Sampling

involves converting the continuous signal to a discrete representation for storage and analysis. The collection hardware is configured to sample the RF frequencies at a sampling rate meeting the requirements of the Nyquist-Shannon theorem [67].

Following near-field probe collection, the analog emission responses are digitally sampled for subsequent storage and post-collection processing. Under Nyquist criteria, the collected analog response must be sampled at a rate of  $f_s \geq 2 \times f_M$ , where  $f_M$  is the maximum frequency extent of the RF response. For emissions collected here, the maximum frequency extent was limited by placing an in-line RF filter between the Riscure near-field probe and the LeCroy oscilloscope (o'scope) used as the receiver. The RF filter bandwidth is determined by the spectral points at which the signal's power (S) is attenuated by  $S_A \leq 3.0\text{dB}$ .

In addition to sampling frequency  $f_s$ , another critical aspect in the sampling process is quantization of TD signal samples. Quantization involves mapping a continuous analog variable (collected RF emission) into a discrete digital variable. The voltage range and *bit-depth* define the analog-to-digital mapping process. For example, an input voltage range of  $V \in [0, 2.55]$  V gets mapped to an 8-bit digital variable and provides the ability to discern between  $2^8=256$  total discrete voltage levels in quantization increments of  $q=2.55/(256 - 1)=0.01$  V. The resultant mapping of a continuous input voltage to a discrete variable inherently introduces *quantization error* into the digitized sample values. The adverse effects of quantization error vary with application and efforts using identical equipment as this research successfully discriminated between hardware devices while experiencing no adverse quantization effects [9–11]. Given this motivation, the effect of quantization error was not addressed or analyzed under this research. The specific bit-depth and sampling rate implemented under this research are discussed in further detail in Chapter 3.

## 2.4 Post-Collection Processing

The primary post-collection processing methods used for this research were based on *Correlation* and the *Hilbert transform*. Collectively, these methods are the basis of the Correlation-Based Anomaly Detection (CBAD) process that is introduced under this research and serves as the core signal processing engine.

*2.4.1 Correlation.* The correlation processing used here extends beyond traditional digital communication system applications and is more consistent with what is commonly used in image processing and other fields requiring signal identification in noisy environments [20]. Given two discrete complex-valued sequences  $x[n]$  and  $y[n]$ , the  $k^{th}$ -lag element of the auto-correlation ( $R_{xx}[k]$ ) and cross-correlation ( $R_{xy}[k]$ ) sequences are given by,

$$R_{xx}[k] = \sum_n x_n x_{n-k}^* , \quad (2.1)$$

$$R_{xy}[k] = \sum_n x_n y_{n-k}^* , \quad (2.2)$$

respectively, where  $*$  denotes the complex conjugate. From an a-posterior probability perspective, classification and verification are related processes that can be independently implemented [11]. However, existing classification processes require considerable resources for a large number of classes and/or class features. Considerable work has been dedicated to quantifying and reducing the computational complexity of such processes [3, 43]. Still, concern remains for implementation using systems having limited or modest computing capability. Correlation-based methods are a less computationally intensive alternative for addressing these concerns and the foundation of optimal matched filtering applications, with one prevalent implementation being the estimation of digital communication symbols [72]. Classification processes vary greatly in the execution cost, but the correlation process operational

cost is predictable and well bounded. The operational performance using two discrete sequences, say  $x[n]$  and  $y[n]$  of length  $N$ , is computable and analytically bounded by

$$\mathcal{O}(R_{XY}[x[n], y[n]]) \sim \mathcal{O}(N^2). \quad (2.3)$$

where  $\mathcal{O}(\cdot)$  denotes the computational time complexity.

*2.4.2 Hilbert Transform.* The Hilbert Transform (HT) is commonly used in audio signal processing applications to stabilize signal amplitude (envelope) estimation [31, 71]. The HT of continuous signal  $x_s(t)$  is given by [30, 32]

$$H(t) = x_s(t) \circledast \frac{1}{\pi t} = \frac{1}{\pi} P.V. \int_{-\infty}^{\infty} \frac{x(\tau)}{t - \tau} d\tau, \quad (2.4)$$

where  $\circledast$  denotes convolution and P.V. denotes the Cauchy principal value. Now letting  $x[n]$  be a periodic sequence of  $N$  consecutive time samples of  $x_s(t)$ , elements of the Discrete Hilbert Transform (DHT) are given by [50]

$$H[n] = \frac{2}{N} \sum_{k \text{ Odd}} x_s(k) \cot\left(\frac{\pi}{N}\right) (n - k); \quad n \text{ Even}, \quad (2.5)$$

$$H[n] = \frac{2}{N} \sum_{k \text{ Even}} x_s(k) \cot\left(\frac{\pi}{N}\right) (n - k); \quad n \text{ Odd}. \quad (2.6)$$

Of importance to this research is that the near-field probe and o'scope collection process described in Sect. 2.3.2 yields real-valued samples of the collected emission. Thus, the DHT process in (2.5) and (2.6) is readily implemented using the MATLAB<sup>®</sup> `hilbert` function. Strictly speaking, the MATLAB<sup>®</sup> `hilbert` function returns a complex *analytic signal* representation with the real In-phase (I) components being the original input sequence and the imaginary Quadrature (Q) components being the input sequence with a 90° phase shift [62]. The imaginary

Quadrature components represent the results of performing the Hilbert transform of the original real sequence. The corresponding instantaneous *amplitude* response of the real-valued input signal is simply found by taking the magnitude of each complex I-Q pair and has the same length as the original sampled response.

## 2.5 Verification-Based Discrimination

The verification-based discrimination process used for this research is consistent with the methodology used for biometric identity verification [48]. As implemented here, the one-to-one verification process includes a comparison the DUT's *current* unknown state (as captured in a current RF fingerprint) with a *stored* reference fingerprint from the same device operating in a known state. This process and fingerprints from untransformed time domain URE signals had been previously used to verify PIC micro-controller operation (software discrimination) and to discriminate between PIC micro-controller ICs (hardware discrimination) [11]. The process in these earlier works was adopted here to support an *anomalous* vs. *normal* assessment methodology. In this case, an anomaly is any type of response, behavior, etc., that is not deemed normal and which may occur as a result of hardware and/or software failure, degradation, or modification; the focus here was on detecting *software* anomalies through verification of the operating condition response.

By implementing the general biometric verification process in support of *hardware* anomaly detection, PIC micro-controller identities have been verified to better than 99.5% accuracy [11]. These previous results increased the envisioned probability of success for the proposed *anomalous* vs. *normal* assessment methodology described in Chapter 3 using more complicated PLC-based SCADA device operations with a goal toward determining the DUTs current operational state. The verification process is implemented by presenting all current observations as normal operation regardless of the actual (unknown) operation and making a final declaration of normal or anomalous. Relative to possible verification outcomes in other verification

and detection work [11,48,83], Table 2.1 shows there are four possible outcomes from the *normal* vs. *anomalous* declaration process. In the context of successful *Anomaly Detection*, the True Anomaly Detection outcome represents success.

Table 2.1: *Normal* vs. *Anomalous* Verification Outcomes: A device’s current operational state is assessed by claiming *Normal* and making a final declaration based on operational credential analysis with a goal of achieving reliable *True Anomaly Detection*.

Actual	Claimed	Declared	Outcome
Normal	Normal	Normal	True Normal Verification
Normal	Normal	Anomaly	False Anomaly Detection
Anomaly	Normal	Normal	False Normal Verification
<b>Anomaly</b>	Normal	<b>Anomaly</b>	True Anomaly Detection

*2.5.1 ROC Performance Assessment.* Quantitative performance assessment of the verification-based *anomalous* vs. *normal* assessment is based on ROC curve analysis as commonly used for binary classification problems such as biometric verification [11,48]. In this case, verification threshold  $t_V$  is set based on training and used to declare (rightly or wrongly) that the current operating condition is *normal* (verification) or *anomalous* (detection). For assessment outcomes in Table 2.1, ROC curves are generated by varying  $t_V$  over its valid range and recording the True Anomaly Detection Rate (TADR) (anomalous conditions correctly declared anomalous) and the False Anomaly Detection Rate (FADR) (normal conditions incorrectly declared anomalous) for each variation in  $t_V$ . The resultant ROC curve is plotted as TADR versus FADR as threshold  $t_V$  varies. The Equal Error Rate (EER) point is the point on the ROC curve at which  $FADR=1-TADR=FNVR$  (False Normal Verification Rate). The EER provides a single metric for comparing two detection methods, with a lower EER indicating a more effective detection method.

### 3. Methodology

This chapter provides details on the methodology implemented to conduct the research and generate results presented in Chapter 4. The Correlation Based Anomaly Detection (CBAD) process is used to detect anomalous Programmable Logic Controller (PLC) operating conditions, with a goal of reliably differentiating between desired *normal* (*Norm*) and undesired *anomalous* (*Anom*) operating conditions. In an operational environment an anomalous operating condition could be triggered by *software* and/or *hardware* failure, degradation, etc. Thus, a single verification-based anomaly detection approach was developed here to support 1) *software anomaly detection*—discriminating between various *operating conditions* to detect malfunctioning or malicious software, firmware, etc., and 2) *hardware component discrimination*—discriminating between various *hardware components* to detect malfunctioning or counterfeit, trojan, etc., Integrated Circuits (ICs).

Software anomaly detection capability is assessed in Chapter 4 using the proposed CBAD process with three specific collected, sampled, and post-collection processed input sequence types: 1) Time Domain (TD) PLC emission sequences 2) Hilbert transformed PLC TD emission sequences, and 3) Radio Frequency Distinct Native Attribute (RF-DNA) feature sequences. Hardware discrimination capability is likewise assessed in Chapter 4 using a Generalized Relevance Learning Vector Quantization-Improved (GRLVQI) process with two specific collected, sampled, and post-collection processed input sequence types: 1) RF-DNA feature sequences extracted from TD PLC sequences, and 2) CBAD Correlation Domain (CD) feature sequences extracted from Hilbert transformed TD PLC sequences. Details for the PLC devices, PLC *Norm* and *Anom* Ladder Logic Programs (LLPs), RF emission collection and processing, and the CBAD and GRLVQI verification process are provided in the following sections.

### 3.1 PLC Device Description

Chapter 4 results are based on experimentally collected RF emissions from  $N_D=10$  Allen Bradley SLC-500 05/02 Central Processing Unit (CPU) PLC devices. The Device Under Test (DUT) to PLC identity (ID) mapping is presented in Table 3.1. The PLC devices are all the same make and model and were chosen for proof-of-concept demonstration given they 1) are readily available commercially, 2) they are prominently used in industry, and 3) their primary Micro Controller Unit (MCU) has similar clock speed and internal data bus structure to other MCU used in previous related efforts [10, 11].

Table 3.1: Device Under Test (DUT) to PLC Identity ID Mapping and Class ID Assignment Based on Device Labeling and Logos.

DUT ID	MCU Label	MCU Logo	PLC ID	Class ID
DUT1	NXP	None	WQ	1
DUT2	NXP	None	WV	1
DUT3	None	Philips	KG	2
DUT4	None	Philips	QI	2
DUT5	Philips	Philips	KV	3
DUT6	Philips	Philips	OV	3
DUT7	Philips	Philips	RG	3
DUT8	None	Philips	ZC	4
DUT9	None	Philips	ZZ	4
DUT10	Signetics & Intel	Signetics	ZA	5

The selected PLC devices are visually discernable and were categorized into classes based on different labeling characteristics. An additional means for qualitatively categorizing devices is through visual analysis of RF emission *spectral intensity*—a graphical representation of maximum Power Spectral Density (PSD). For assessment here, spectral intensity plots were generated by collecting  $N_B=400$  emissions from each device executing an arbitrary LLP using a Low Pass Filter (LPF) to mitigate aliasing effects. The LPF had an effective bandwidth of  $W_{LP}\approx 81.0$  MHz. Considering an arbitrary sampled TD sequence having  $N_s$  total samples,  $x[n]=\{x[n_i], x[n_2], \dots, x[n_{N_s}]\}$ , the corresponding PSD components  $|X[n]|$  can be obtained using



a Discrete Fourier Transform (DFT) given by [72],

$$X[n] = \frac{1}{N_s} \sum_{k=1}^{N_s} x[n] e^{-j\Phi(N_s, k, m)} : 1 \leq m \leq N_s , \quad (3.1)$$

where

$$\Phi(N_s, k, m) = \left( \frac{2\pi}{N_s} \right) (k-1)(m-1) : 1 \leq m \leq N_s . \quad (3.2)$$

The PLC spectral intensity plots ( $20 \times 20 \max[|X[n]|]$  values) were generated using (3.1) and (3.2) for all  $N_D=10$  devices using  $N_B=400$  total emission collections, with one emission collected from each of  $(N_X=20) \times (N_Y=20)=400$  uniformly spaced points on a rectangular grid over the DUT surface. The resultant spectral intensity plots are shown in Fig. 3.1 and provide an alternate, qualitative means of assigning DUTs to classes. Each point on the 2D plots represents the  $\max[|X[n]|]$  of the PSD series associated with the emission collected at that location. Note that Device *RG* is assigned to *Class 3* based on DUT markings in Table 3.1, but bears a closer resemblance to devices in *Class 1* when considering its spectral intensity in Fig. 3.1.

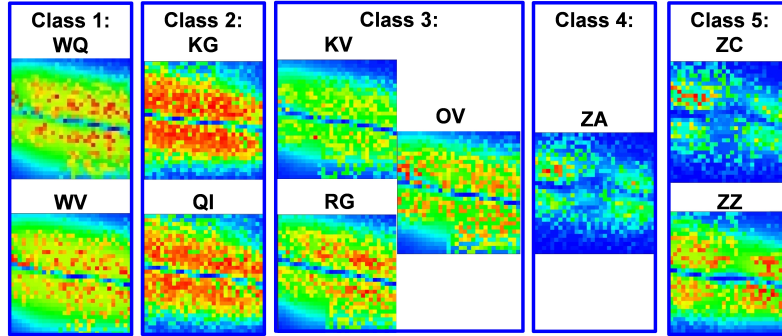


Figure 3.1: Spectral intensity plots generated as emission maximum PSD responses over a  $20 \times 20$  uniform grid above the PLC MCU surface. Plots enable qualitative device classification base on visual analysis of emission characteristics. With one exception, responses here confirm the PLC class assignments in Table 3.1 which are based on device label markings; the *RG* PLC response here is visually more consistent with *Class 1* vs. the *Class 3* table assignment.

### 3.2 PLC Operating Conditions

PLC emissions were collected for a single *Norm* and two *Anom* operating conditions using the experimental LLPs shown in Fig. 3.2. Prior to collecting PLC responses using the methods described in Sect. 3.4, the PLC devices were pre-programmed with the desired LLP which was then executed repeatedly until halted through user intervention. Two major LLP variants were implemented for demonstration, including an 1)  $N_{OP}=5$  version and 2)  $N_{OP}=10$  version for each of the *Norm*, *Anom* #1 and *Anom* #2 operating conditions (six total LLPs). The LLPs were executed repeatedly and emissions collected from the PLC until power was turned off or execution was terminated through user intervention.

*3.2.1 Ladder Logic Program:  $N_{OP}=5$ .* The first LLP variant is used to demonstrate the feasibility of CBAD processing using  $N_{OP}=5$  LLP operations and consists of a specific order of Move (*MOV*) and Square-Root (*SQR*) commands that operate on data within the PLC memory. While not graphically illustrated, the results after each executed operation are saved to registers within the PLCs before the next operation is executed. As shown in Fig. 3.2, the anomalous operating condition programs were generated from the *Norm* operating condition program by reordering (*Anom* #1) and replacing (*Anom* #2) specific operations. These anomalous program conditions are intended to mimic potentially disruptive and/or malicious alterations as shown in . As seen in Fig. 2(a), the *Norm* LLP consists of alternating *MOV* and *SQR* operations:  $\{MOV, SQR, MOV, SQR, MOV\}$ . These were chosen to contrast a relatively short operation (*MOV*) with a more computational demanding operation (*SQR*) in an effort to simplify the first attempt at detecting software anomalies.

The *Anom* #1 operating condition LLP was created by reordering the  $N_2=2^{nd}$  and  $N_3=3^{rd}$  operations. The resulting LLP consists of:  $\{MOV, MOV, SQR, SQR, MOV\}$ . The *Anom* #2 operating condition LLP was created by replacing the

$N_4=4^{th}$  operation (*SQR*) with a *MOV* operation. The resulting LLP consists of:  $\{MOV, SQR, MOV, MOV, MOV\}$ .

*3.2.2 Ladder Logic Program:  $N_{OP}=10$ .* The second LLP variant consists of  $N_{OP}=10$  total PLC operations and includes a specific order of Move (*MOV*), Square-Root (*SQR*), Add (*ADD*), Multiply (*MUL*), Subtract (*SUB*), Divide (*DIV*), Negate (*NEG*), Convert To Binary Coded Decimal (*TOD*), and Convert From Binary Coded Decimal (*FRD*) commands that operate on data within the PLC memory. While not graphically illustrated, the results after each executed operation are saved to registers within the PLCs before the next operation is executed. The operations were selected to exercise the available math functions for the selected PLCs. As shown in Fig. 3.2, the anomalous operating condition programs are generated from the *Norm* operating condition program by reordering (*Anom #1*) and replacing (*Anom #2*) specific operations. These anomalous program conditions are intended to mimic potentially disruptive and/or malicious alterations as shown in Fig. 3.2.

The *Anom #1* operating condition LLP was created by reordering the  $N_5=5^{th}$  and  $N_6=6^{th}$  operations. The resulting LLP consists of:  $\{MOV, SQR, ADD, MUL, DIV, SUB, NEG, TOD, FRD, SQR\}$ . The *Anom #2* operating condition LLP was created by replacing the  $N_4=4^{th}$  operation (*MUL*) with an *ADD* operation. The resulting LLP consists of:  $\{MOV, SQR, ADD, ADD, SUB, DIV, NEG, TOD, FRD, SQR\}$ .

### 3.3 CBAD Processing Overview

The CBAD process was implemented as illustrated in Fig. 3.3 and used to perform verification-based anomaly detection using five distinct sub-processes:

1. RF Emission Collection—emissions are collected from each PLC operating under *Norm* and/or *Anom* conditions as required to support both *software anomaly detection* and *hardware component discrimination* assessment.

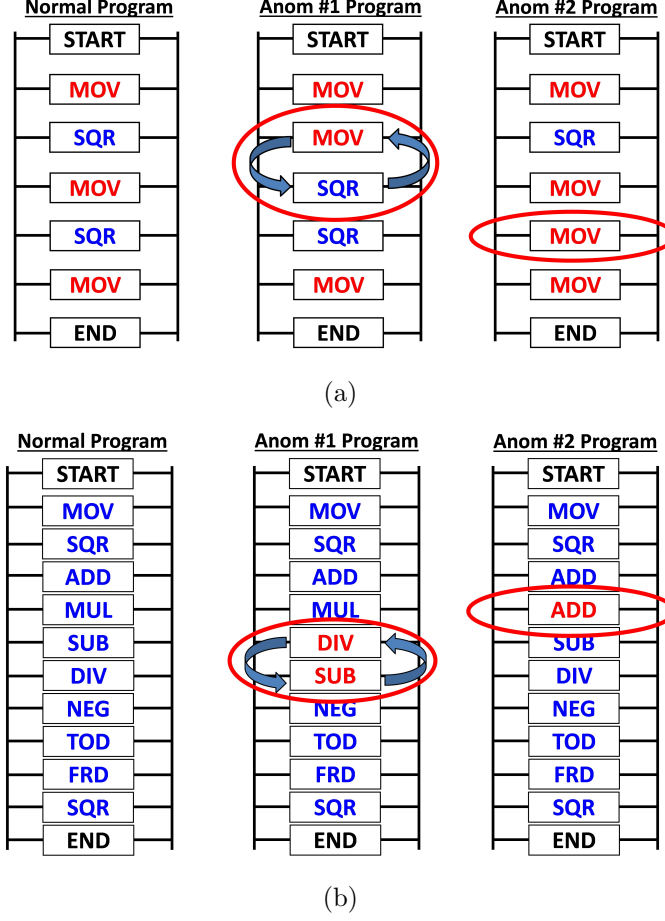


Figure 3.2: Normal (*Norm*) and Anomalous (*Anom*) ladder logic programs for (a)  $N_{OP}=5$  and (b)  $N_{OP}=10$  operating conditions. Anomalous conditions are induced through *reordering* (*Anom #1*) and *replacement* (*Anom #2*) of selected operations.

2. Data Segregation—sequences are divided into independent “Training” ( $x_{Tng}[n]$ ) and “Testing” ( $x_{Tst}[n]$ ) sets; this distinction is adopted here for consistency with terminology used in the pattern recognition community [22].
3. Normal Reference Sequence Generation—normal reference sequence  $x_N[n]$  in Fig. 3.3 is generated using *Normal* “Training” data in  $x_{Tng}[n]$ .
4. Cross-Correlation  $C_{NC}[k]$  Generation— $C_{NC}[k]$  is generated using the selected  $x_N[n]$  reference sequence and a given *Collected* sequence  $x_C[n]$  to be verified.

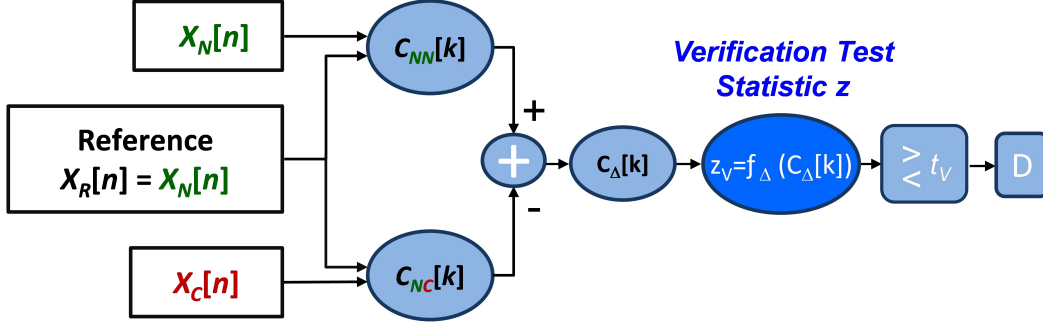


Figure 3.3: Correlation-Based Anomaly Detection (CBAD) process for verifying that the *Current* unknown sequence  $X_C[n]$  is a result of either a) *Normal* operating conditions (declared when  $z_V \leq t_V$ ) or b) *Anomalous* operating conditions (declared  $z_V > t_V$ ). The *claimed* condition is always normal and implemented using a correlation reference of  $X_R = X_N$  [89].

5. Verification Test Statistic Generation—verification test statistic  $z_V$  is generated using a selected Difference Function  $f_{\Delta}$  and correlation Difference  $C_{\Delta}[k]$ , i.e.,  $z_V = f_{\Delta}(C_{\Delta}[k])$ .
6. Establish Verification Threshold—verification threshold  $t_V$  is determined and set using CBAD “Training” statistics  $\{z_V[n]\}$  under *Norm* operating conditions.
7. Verification Declaration—test statistic  $z_{V_{Tst}}$  is compared with the established verification threshold  $t_V$  and a declaration made such that  $z_{V_{Tst}} \leq t_V \rightarrow \text{Norm}$  and  $z_{V_{Tst}} > t_V \rightarrow \text{Anom}$ .

More details for each of these CBAD processing steps are provided in Sect. 3.8.

### 3.4 RF Emission Processing

Experimentally collected PLC emissions were used to form required input sequences for CBAD and RF-DNA processes. RF emissions were collected using a Riscure RF probe attached to a LeCroy 804Zi Oscilloscope. All DUT RF emissions were collected at sample frequency of  $f_s = 250$  MSps using a near-field probe having a baseband bandwidth of  $W_{BB} = 500$  MHz. Following the collection and sampling of

the emissions, they are post-collection processed using MATLAB<sup>®</sup> functions. The processing includes filtering, downconverting, and decimating the emissions prior to using the emissions as input sequences for the CBAD process. The following sections provide details related to the processing and collection of the RF emissions.

*3.4.1 Collection and Sampling.* The frequency of interest for the RF collections against URE devices in previous research efforts had been selected based on the harmonics of the clock frequency for the target devices [10,11]. The observed MCU clock frequency in the Allen Bradley PLCs was  $f_{CLK}=18.5$  MHz, with the strongest frequency component spectrally aligned with a clock harmonic. As seen in Fig. 3.4, this component is manifest near the  $H_{CLK}=3^{rd}$  MCU clock harmonic for the Allen Bradley PLCs considered and has a targeted collection frequency of  $f_c=55.5$  MHz. To ensure the targeted signal frequency is collected in compliance with Nyquist cri-

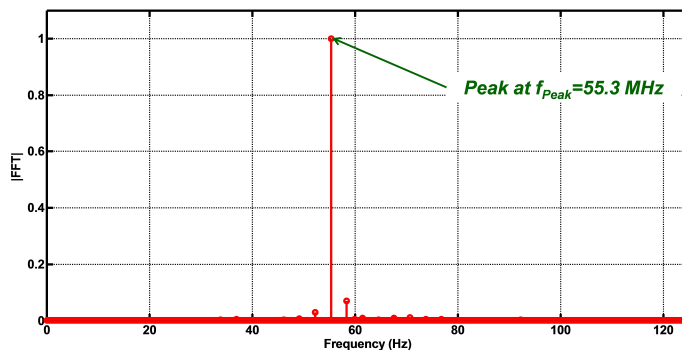


Figure 3.4: Representative normalized PSD for the PLC *WQ* device showing a distinct peak response at  $f \approx 55.3$  MHz.

teria, the signal is sampled at a rate of  $f_s=250$ MSps. To minimize aliasing caused by frequency components  $f \geq 125$  MHz, the signal is filtered after collection by the RF probe and prior to sampling using a passive inline LPF having a cutoff frequency of  $f_{CO}=81.0$  MHz such that all frequency components greater than  $f_{CO}$  are attenuated by 3.0dB or greater. The attenuation for frequency values of interest is shown in Fig. 3.5. The collected, filtered, sampled RF emission is stored as a sequence of real values representing the measured voltage of the signal as sampled at each time

region. The real values are stored as 8-bit integers. The signal collection and storage process, from collecting using the RF probe, to storage as integer sequences is performed in real-time. Following the collection and storage, the signals are processed using MATLAB<sup>®</sup> prior to being used as inputs for the CBAD process.

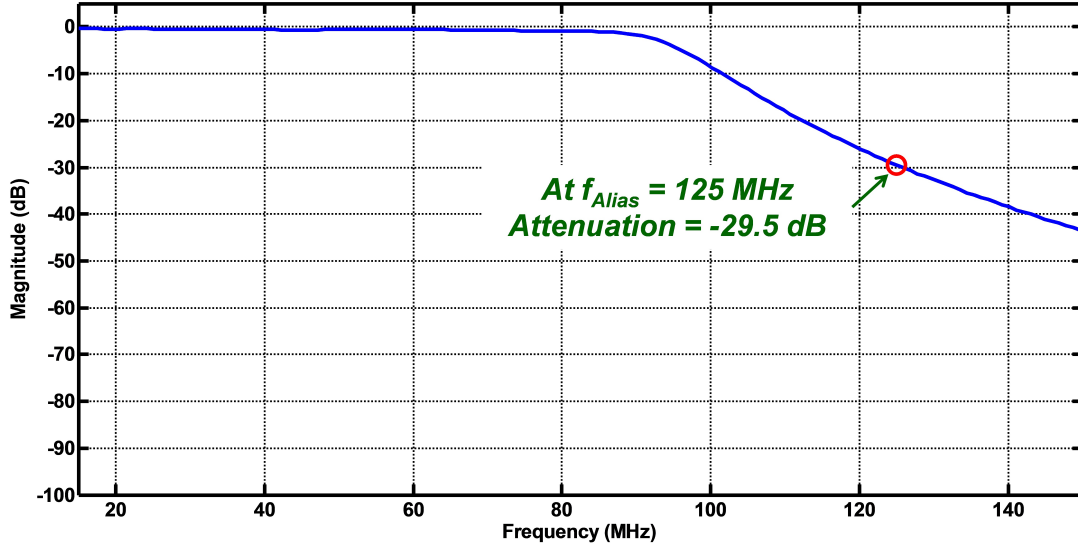


Figure 3.5: Impulse frequency response of the  $f_{CO}=81.0$  MHz LPF. The filter is designed to mitigate adverse aliasing effects by attenuating frequency components above  $f \approx 125$  MHz by at least 29.5dB.

*3.4.2 PLC Mainboard Mounting.* Prior to emission collection, the DUT must be placed in a position such that the near-field probe can be placed in close proximity to the MCU on the PLC Mainboard. The PLCs, as manufactured, do not provide space for placement of the probe due to obstruction caused by the casing. All mainboards were removed from their casing for the purpose of this research effort. The entire PLC device plugs into a backplane, which provides power and communication between PLC modules. In order to provide room to place the probe, the PLC mainboards are connected to the backplane using a set of extension cables. All PLCs are connected using the same set of cables, which must be unplugged from one DUT and plugged into the next between DUT emission collections. The PLC mainboards are placed on a probe table providing support for the mainboard and

the ability to move the probe in three dimensions spatially. The probe table provides precise placement of the probe, but does not have a native ability to repeat probe placement positions between collections. A probe placement routine was used to reliably place the probe prior to each collection. The probe placement routine is discussed in Sect. 3.4.3. The collection configuration can be seen in Figure 3.6.

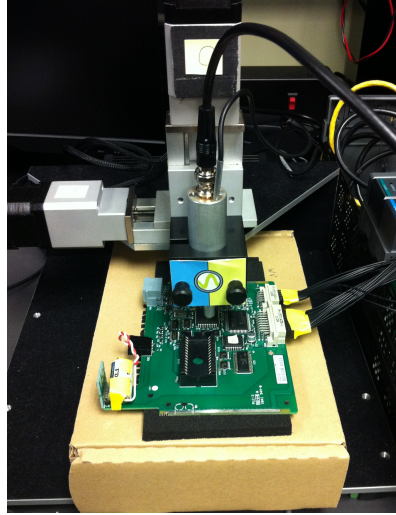


Figure 3.6: Picture of XYZ near-field probe station used for collecting PLC emissions.

*3.4.3 RF Near-Field Probe Placement.* Course near-field probe placement was determined once per DUT during initial testing and physically marked for repeated placement during subsequent collections. The alignment to a physical marker is not precise enough to avoid altering the collected emissions between collection sessions where the DUT must be removed from the probe table and replaced for collection. Probe placement was performed through a two step process that included 1) Course Placement—the probe is placed a predetermined location on the device surface, and 2) Refined Placement—the probe is repositioned based on RF emission analysis.

The physical location is defined on each device such that the same position is used for every device relative to each device’s physical attributes. To limit the variation between collection locations on the devices, the probe is placed in a location



such that two lines, parallel to the physical edges of the PLC MCU, but perpendicular to each other, are tangential to the edge of the probe. Figure 3.7 shows the physical location where the probe is placed.

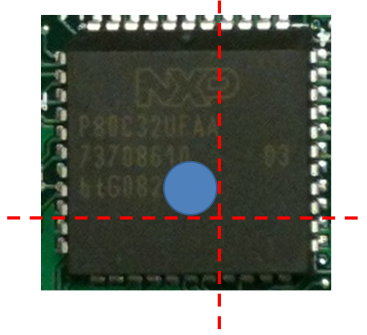


Figure 3.7: The red perpendicular lines are tangent to the near-field probe (blue dot) and identify the location used for PLC MCU emission collection.

The specific probe placement is determined by collecting emissions at  $N_L=100$  locations on a  $(D_X=10) \times (D_Y=10)$  dimensional grid over a  $(x_m=0.75 \text{ cm}) \times (y_m=0.75 \text{ cm})$  square region on the MCU surface. At each location  $i$ , a single alignment location sequence  $x_{a_i}[n]$  is collected. The sequence is collected during the PLC execution or scan of an *alignment LLP*. The alignment LLP uses the *MOV* and *SQR* PLC operations. The alignment LLP consists of an ordered sequence of  $N_{OP}=6$  PLC operations:  $\{MOV, SQR, MOV, SQR, MOV, SQR\}$ . The collected sequences are processed using the same process and method as is implemented for the post-collection processing detailed in Sect. 3.5. The details of the processing are not critical to the understanding of the probe placement routine, but it is important to note that they match those implemented during the training and testing of the CBAD Process.

Recall the alignment LLP consists of alternating *MOV* and *SQR* operations. An *alignment reference LLP* is used in conjunction with the alignment LLP to select the probe position prior to collecting emissions from the PLC MCU. The alignment reference LLP consists of a single *MOV* and *SQR* operation. The sampled, discrete alignment reference signal  $x_R[n]$  is collected while the reference LLP is executed by

the PLC and it represents a single scan of the alignment reference LLP. While there are  $N_L=100$  alignment sequences,  $\{x_{A1}[n], x_{A2}[n], \dots, x_{A100}[n]\}$ , there is only a single alignment reference signal  $x_R[n]$ .

Correlation was the foundation of this research and plays a critical role in nearly every aspect of CBAD processing, including probe placement and alignment. The correlation process is analytically described from a random process perspective in Sect. 2.4.1. For the purpose of this research a tailored correlation process is implemented. Considering two real-valued discrete input sequences,  $x[n]$  having  $N_x$  samples and  $y[n]$  having  $N_y$  samples with  $N_y \leq N_x$ , the  $j^{th}$  element of cross-correlation sequence  $C_{xy}[k]$  as implemented in this research is calculated as

$$C_{xy}[k_j] = \sum_{i=1}^{N_x} x[n_i] \cdot y[n_{j+i}] \quad : \quad 1 \leq j \leq N_y - N_x \quad . \quad (3.3)$$

An automated, repeatable approach for evaluating responses from the  $N_L=100$  probe locations on the DUT was needed to select a location that was best-suited for emission collections. The evaluation criteria are derived from the aligned correlation sequence  $C_{A_i}[k]$  resulting from the correlation process equation (3.3) using the  $i^{th}$  alignment emission  $x_{a_i}[n]$  and the alignment reference emission  $x_R[n]$  as inputs. For the  $i^{th}$  alignment sequence  $x_{A_i}[n]$  having  $N_a$  samples and reference emission  $x_R[n]$  having  $N_r$  samples, the  $j^{th}$  element of the  $i^{th}$  alignment correlation sequence  $C_{A_i}$  for the  $i^{th}$  probe location is calculated as

$$C_{A_i}[k_j] = \sum_{i=1}^{N_r} x_R[n_i] \cdot x_{A_i}[n_{j+i}] \quad : \quad 1 \leq j \leq N_a - N_r \quad . \quad (3.4)$$

Correlation sequence peaks provide a measure of performance for each potential probe position. The alignment reference LLP sequence  $x_R[n]$  consists of a single  $\{MOV, SQR\}$  sequence as compared to the three  $\{MOV, SQR\}$  sequences in the alignment LLP sequence  $x_A[n]$ . For each emission collected,  $N_P=3$  peaks are ex-

pected in the  $C_A[k]$  sequence given that the alignment LLP consists of the reference LLP repeated  $N_P=3$  times. The probe position on the  $(D_X=10)\times(D_Y=10)$  dimensional grid was selected based on a voting process that considers three values for each of the  $N_L=100$  alignment correlation sequences: 1) the maximum correlation value, 2) the mean value of the highest  $N_P=3$  correlation peaks, and, 3) the sum of the highest  $N_P=3$  correlation peaks. A probe position producing the highest value for two of the three criteria is used as the position for emission collection. For cases when no single emission satisfies this criteria, the probe position yielding the maximum mean correlation of the highest three peaks is used.

*3.4.4 PLC LLP Triggering.* A *trigger* was used to initialize RF emission collections based on a Light Emitting Diode (LED) output voltage ( $V_{LED}=5.0$  V) assigned as a physical PLC register output during the first *MOV* operation in each LLP. This output was toggled during each scan by a square wave having an approximate 50% duty cycle and scan frequency of  $f_{Scn}=1/(2\times T_{Scn})$  where  $T_{Scn}$  is the approximate time it takes to complete a single LLP scan. Both the leading and trailing edge of the square wave were used as a trigger. Since the PLC outputs are assigned at the end of a scan, the triggered collections actually began just prior to the start of a subsequent scan with square wave period ( $T_{Scn}$ ) providing an approximate measure of collected scan duration.

### 3.5 Post-Collection Processing

Following the collection, sampling, and storage the emissions are post-collection processed using MATLAB<sup>®</sup>. Before the post-collection process can begin the sequences are converted from the native Riscure Inspector<sup>®</sup> software format to a MATLAB<sup>®</sup> compatible format. This is accomplished using code developed in support of previous AFIT Unintentional Radiated Emission (URE) research efforts [9]. The code was implemented in its original, unaltered state and so is not discussed in detail for this research effort.

Once the collected emissions are converted to a MATLAB<sup>®</sup> compatible format, post-collection processing can be performed using four primary steps: 1) down-conversion to an Intermediate Frequency (IF), 2) digital bandpass filtering, 3) down-sampling using proper decimation, and 4) applying the selected transform to obtain the final sequence used for verification. Each of these processes are described in greater detail in the following sections.

*3.5.1 Down-Conversion and Bandpass Filtering.* Following collection and storage of the input sequences, the signals were processed using MATLAB<sup>®</sup> to isolate specific frequency components of interest, down-convert the signals to near-baseband, and properly decimate to signals to reduce computational overhead of subsequent processing. The emissions were digitally filtered after collection using an 8<sup>th</sup>-order Butterworth bandpass filter with a center frequency of  $f_{BP}=55.5$  MHz and  $-3.0$  dB bandwidth of  $W_{BP}=1.0$  MHz. The frequency response of the filter is presented in Fig. 3.8. The center frequency was empirically selected based on observing emissions

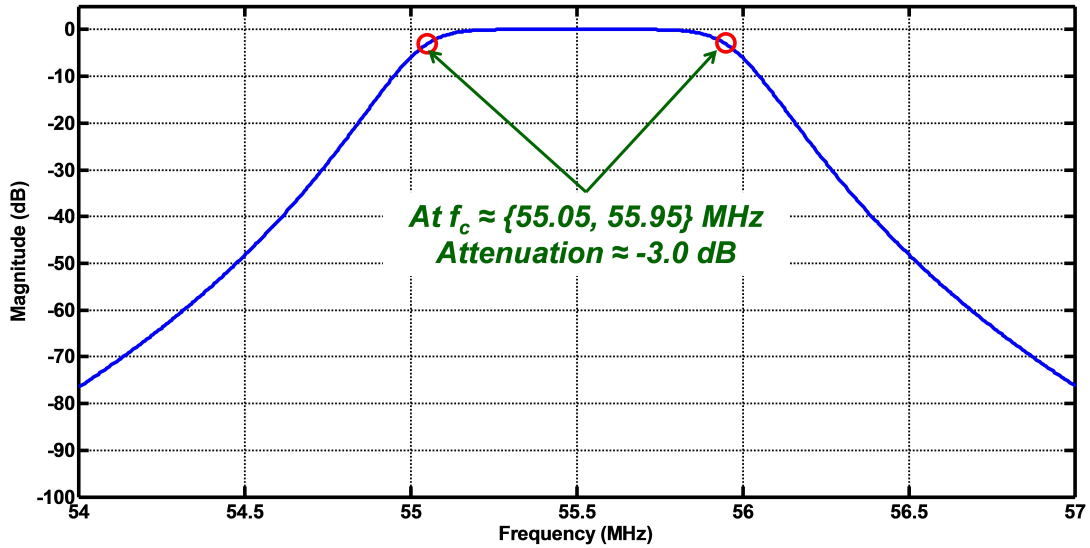


Figure 3.8: Impulse frequency response of the digital 8<sup>th</sup>-order Butterworth bandpass filter having a center frequency of  $f_{BP} \approx 55.5$  MHz and a  $-3.0$  dB bandwidth of  $W_{BP} \approx 1.0$  MHz.

from all PLC devices as the third MCU clock harmonic ( $f_c=3\times f_{CLK}=55.5$  MHz). The center frequency and bandwidth were selected based on analysis of center frequencies  $f_c=\{18.5, 37.0, 55.5, 74.0\}$  MHz as aligned to the first four clock harmonics for the observed MCU clock frequency  $f_{CLK}=15.5$  MHz and  $-3.0$  dB bandwidths of  $BW_{BP}=\{1.0, 2.0, 3.0, 4.0, 5\}$  MHz. The analysis demonstrated that the selected bandwidth and center frequency provided the best performance in accurately discriminating between the *MOV* and *SQR* PLC operations. Operation discrimination performance was assessed using the CBAD process to generate test statistics with a single training reference sequence and multiple test sequences from the  $N_D=6$  PLCs that were initially purchased to support the research effort; these are the *WQ*, *WV*, *RG*, *KG*, *KV*, *QI* devices identified in Table 3.1.

*3.5.2 Sub-Sampling/Proper Decimation.* Based on spectral analysis and in accordance with Nyquist criteria, the down-converted bandpass TD responses were properly decimated by a factor of 20 to produce sub-sampled sequences at  $f_s=12.5$  MSps for post-collection processing. By down-converting the filtered signal to  $f_{IF}=2.0$  MHz, the original signal content in  $f\in[55.0, 56.0]$  MHz is relocated to a down-converted range of  $f\in[1.0, 3.0]$  MHz. With the frequency content of interest centered at  $f_{IF}=2.0$  MHz, the signal was filtered using a LPF having a  $-3.0$  dB cutoff frequency of  $f_{LPF}=3.5$  MHz and the impulse response seen in Fig. 3.9. The filtered signal is decimated by a factor of 20, reducing the number of signal samples yielding a final sampling rate of  $f_s=12.5$  MSps for the down-converted signal.

*3.5.3 Signal-to-Noise Ratio Scaling.* The experimentally collected emissions consisted of two components, including the 1) desired signal component  $x_s[n]$ , and an 2) undesired background noise component  $x_B[n]$ . It was assumed the signal and noise components are independent and that  $x_s[n]$  is generally *deterministic* and  $x_B[n]$  is a *random* process; under these assumptions the collected response  $x_C[n]=x_s[n]+x_B[n]$  is a random process. One research objective involved assessing

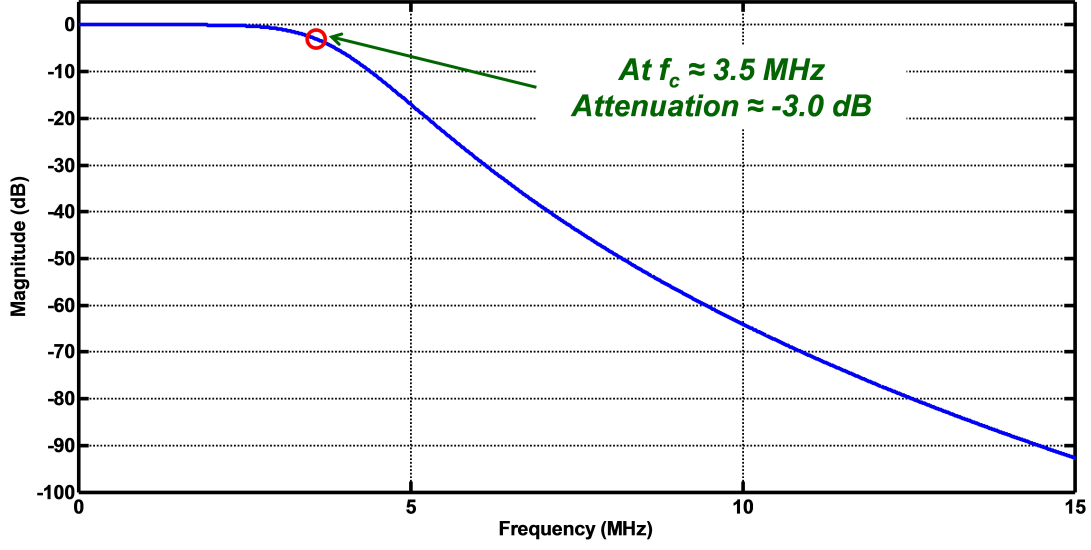


Figure 3.9: Impulse frequency response of the digital 8<sup>th</sup>-order Butterworth LPF having a  $-3.0\text{dB}$  bandwidth of  $W_{LP} \approx 3.5$  MHz.

verification-based anomaly detection performance under varying  $SNR$  conditions given that  $SNR$  variation commonly occurs in operational environments given inherent RF channel variation between the RF source and collection receiver. The  $SNR$  is calculated as the ratio of average signal power ( $P_s$ ) to average noise power ( $P_N$ ) expressed in Decibels (dB).

To mitigate the need for repeated emission collections at varying distances and channel conditions, the  $SNR$  variation effects were simulated by adding like-filtered, power scaled Additive White Gaussian Noise (AWGN) noise realizations  $x_N[n]$  to as-collected, filtered PLC emissions  $x_C[n]$ . The resultant “as evaluated” sequence that is used for performance assessment and analysis is given by  $x_A[n] = x_s[n] + x_B[n] + x_N[n]$  where  $x_N[n]$  has been appropriately power-scaled to achieve the desired analysis  $SNR_A$ . The average power in an arbitrary complex sequence  $y[n]$  having  $N_y$  can be estimated using,

$$P_y \approx \frac{1}{N_y} \sum_{i=1}^{N_s} y[n_i] y[n_i]^* , \quad (3.5)$$

where  $*$  denotes complex conjugate. When  $y[n]$  is real-valued (3.5) becomes,

$$P_y \approx \frac{1}{N_y} \sum_{i=1}^{N_s} y[n_i]^2 . \quad (3.6)$$

Considering that real-valued PLC collections were used for this research, the expression in (3.6) was appropriate for calculating required average powers and AWGN power scale factors. Given a desired  $SNR_A$  with  $x_A[n]=x_s[n]+x_B[n]+x_N[n]$  representing the analysis sequence, the average power in  $x_A[n]$  and its components can be calculated using (3.5) and are denoted by  $P_A$ ,  $P_s$ ,  $P_B$ , and  $P_N$  for the respective  $x_A[n]$ ,  $x_s[n]$ ,  $x_B[n]$ , and  $x_N[n]$  sequences. Assuming all components of  $x_A[n]$  are independent, the total average power in  $x_A[n]$  is  $P_A=P_s+P_B+P_N$  and  $SNR_A$  can be calculated using

$$SNR_A = P_s/(P_B + P_N) . \quad (3.7)$$

Given that  $P_s$  and  $P_B$  can be estimated for experimentally collected emissions, the  $SNR_A$  expression in (3.7) is used to solve for the required  $P_N$  in  $x_N[n]$  using

$$P_N = (P_s/SNR_A) - P_B , \quad (3.8)$$

which in turn is used to calculate the corresponding power scale factor for AWGN noise realizations, i.e.,  $x_N[n] \approx \sqrt{P_N} x_{AWGN}[n]$  for  $x_{AWGN}[n] : N[0, 1]$ .

Each collection of “as evaluated”  $x_A[n]$  analysis sequences at  $SNR_A$  that are input to the CBAD process was generated using a total of  $N_{Nz}$  independent, like-filtered AWGN realizations for  $x_N[n]$ . Thus, for a performance assessment based on  $N_B$  collected emission sequences  $\{x_{C1}[n], x_{C2}[n], \dots, x_{CN_B}[n]\}$  there are a total of  $N_Z=N_B \times N_{Nz}$  sequences used for each  $SNR_A$  considered.

### 3.6 Sequence Transformation

Prior to inputting sequences into the CBAD process, the sequences are transformed using one of three methods implemented under this research: 1) an absolute value function, 2) a Hilbert transform function, and 3) an RF-DNA transform. In addition, the resultant absolute value and Hilbert transform sequences are normalized to produce  $\bar{x}[n]$  which is input to the CBAD process. For sequence  $x[n]$ , normalization of the  $i^{th}$  element is given by

$$\bar{x}[n_i] = \frac{x[n_i]}{\max(x[n])} . \quad (3.9)$$

The absolute value function is the simplest and transforms a given emission sequence,  $x[n]$ , by computing the magnitude of each sequence element. This process is well-known and does not warrant additional discussion. The Hilbert transform and RF-DNA Transform methods are more complicated and discussed further in the following sections.

*3.6.1 Hilbert Transform.* The CBAD verification process is agnostic to what the sequence elements represent and the above process is applicable for all real-valued sequences  $x[n]$ . Thus, the sequences can be generated as either the magnitude of untransformed real valued TD sequences ( $|x[n]|$ ) or as the magnitude of Hilbert transformed TD responses ( $|H[x[n]]|$ ). The transition to  $|H[x[n]]|$  sequences was motivated by previous research showing that anomaly detection capability using  $|x[n]|$  sequences is negatively impacted by cross-collection variance in RF emissions. The observed misalignment (cross-collection time registration) of data sets was often less than  $\pm 10$  TD samples, yet resultant variation degraded verification performance considerably. Thus, as in audio signal processing applications the Hilbert transform is used to stabilize signal's amplitude estimates, [32, 71].

Recall the frequency components of interest are constrained in a frequency range centered around  $f_c=55.5$  MHz with a bandwidth of  $W_{BW}=1$  MHz. Similar to



the work in [101], the Hilbert transform provides a means of estimating an amplitude envelope for a narrowly determined frequency range. The amplitude estimate sequence is obtained from the Hilbert transformed sequence by calculating the magnitude of the complex pair representing each element of the Hilbert transformed sequence. The Hilbert transform in (2.4) effectively shifts the phase of a continuous signal by  $\phi=\pi/2$  radians for all frequency components. The MATLAB<sup>®</sup> `hilbert` function is used to generate the transformed discrete sequence  $H[x[n]]$  for a given real-valued sequence  $x[n]$ . The `hilbert` function in MATLAB<sup>®</sup> returns a complex time analytic representation of the signal having In-phase (I) and Quadrature (Q) components. The magnitude response of a discrete Hilbert sequence  $|H[x[n]]|$  represents the *instantaneous amplitude* or *envelope* of the discrete sequence  $x[n]$ . The input sequence to the CBAD process is the magnitude of the Hilbert Transformed sequence  $|H[x_s[n]]|$ , which is the same length as the TD sequence  $x[n]$ . Consider a Hilbert transformed sequence generated using the `hilbert` function,  $H[x_s[n]]$ . Any element  $H[x_s[n_i]]$  of the sequence consist of both real,  $H_{re}[x_s[n]]$  and imaginary,  $H_{im}[x_s[n]]$  components representing the In-Phase and Quadrature components of the real signal. The amplitude estimate sequence  $|H[x[n]]|$  is defined for any element  $|H[x[n_i]]|$  by calculating the 2-norm with each real-imaginary pair considered a vector

$$\begin{aligned} |H[x[n_i]]| &= || < H_{re}[x_s[n_i]], H_{im}[x_s[n_i]] > ||^2 \\ &= \sqrt{(H_{re}[x_s[n_i]])^2 + (H_{im}[x_s[n_i]])^2} \end{aligned} \quad (3.10)$$

A representative magnitude TD  $|x[n]|$  sequence is shown in Fig. 3.10 along with its corresponding magnitude  $|H[x[n]]|$  sequence.

**3.6.2 RF-DNA Transform.** The RF-DNA transform was implemented according to the process in [9, 21, 39, 58, 76, 102] and was used in this research to reduce the dimensionality of the input sequences and identify those signal attributes

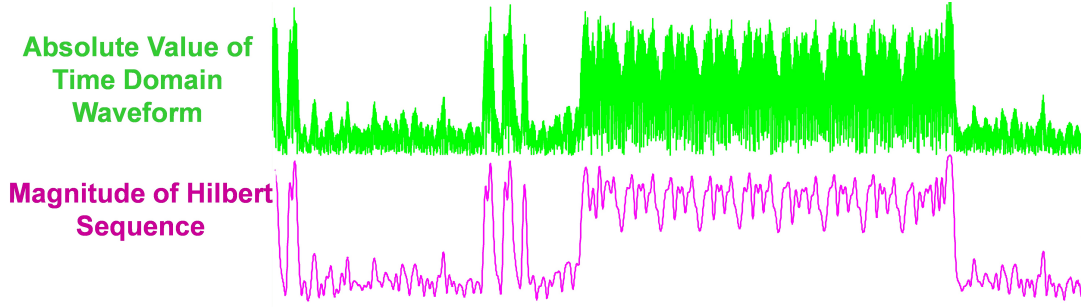


Figure 3.10: Representative responses for the first two LLP operations (*SQR* and *MOV*) under *Norm* operating conditions: (Top) Magnitude of TD  $|x[n]|$  sequence and (Bottom) corresponding Magnitude of Hilbert transform  $|H[x[n]]|$  sequence.

that aid in the discrimination of hardware devices. The RF-DNA transform is a mechanical process calculating sequence attributes without reliance or dependance on the source of the sequence. It has been used previously on sequences representing TD, Spectral Domain (SD), and Time-Frequency (T-F) sequences [11, 42, 81]. For the purpose of this research effort, the RF-DNA was performed on TD emissions only.

RF-DNA reduces the dimensionality of the TD sequences by calculating statistical values (standard deviation  $\sigma$ , variance  $\sigma^2$ , skewness  $\gamma$ , and kurtosis  $\kappa$ ) for instantaneous sequence attributes (amplitude  $a$ , phase  $\phi$ , frequency  $f$ ) over  $N_R$  specified signal regions for an arbitrary input sequence  $x[n]$ . Features are calculated for each specified region of the sequence and concatenated together to form an RF-DNA *fingerprint*  $\mathbf{f}_{TD}$  representing the entire sequence  $x[n]$ .

Each collected DUT emission collected for this research was stored as a real-valued TD sequence  $x[n]$ . Given that the RF-DNA process is inherently base on complex IQ input sequences, the collected  $x[n]$  here were converted to complex IQ sequences of the form  $x_{IQ}[n] = x_{re}[n] + jx_{im}[n]$  using the `hilbert` function in MATLAB®. Composite RF-DNA fingerprints were generated from selected sequences using the following steps:

1. A given sequence  $x_{IQ}[n]$  is divided into  $N_R$  equal length contiguous subregions.

2. Within a given subregion, the mean  $\mu$  value is calculated and subtracted from all subregion samples to minimize the impact of collection bias.
3. The desired instantaneous feature sequence(s) (phase  $\phi[n]$ , amplitude  $a[n]$ , and/or frequency  $f[n]$ ) is calculated for the subregion samples.
4. Selected statistical attributes of standard deviation  $\sigma$ , variance  $\sigma^2$ , skewness  $\gamma$ , and/or kurtosis  $\kappa$  are calculated using all samples within the subregion.
5. The resultant statistical attributes are concatenated to form a single *Regional Fingerprint* sequence with elements arranged in order of signal feature and statistical attribute.
6. Steps 2-4 are repeated for each subregion of  $x[n]$  and the  $N_R$  *Regional Fingerprint* sequences are concatenated to form the *Composite Fingerprint* sequence for  $x[n]$ .

The following sections provide more detail for each of the processes used to generate a *Composite Fingerprint* sequence for a TD  $x_{IQ}[n]$  sequence.

*3.6.2.1 Instantaneous Feature Calculation.* The first step in generating an RF-DNA fingerprint from a TD signal is calculation of selected instantaneous signal features for the sampled TD signal. For the element  $x_{IQ}[n_i] = x_{re}[n_i] + x_{im}[n_i]$ , the instantaneous  $a[n_i]$ , phase  $\phi[n_i]$ , and frequency  $f[n_i]$  sequence elements were calculated using [103]

$$a[n_i] = \sqrt{x_{re}^2[n_i] + x_{im}^2[n_i]} , \quad (3.11)$$

$$\phi[n_i] = \tan^{-1} \left[ \frac{x_{im}[n_i]}{x_{re}[n_i]} \right] , \quad x_{re}[n_i] \neq 0 , \quad (3.12)$$

$$f[n_i] = \frac{1}{2\pi} \left[ \frac{d\phi[n_i]}{dn_i} \right] , \quad (3.13)$$

where  $1 \leq i \leq N_x$  and  $N_x$  is the total number of elements in  $x_{IQ}[n]$ .

For consistency with previous research, the TD sequences in (3.11)–(3.13) are centered and normalized using (3.9); centering simply removes the sequence mean ( $\mu$ ) prior to normalization. The  $i^{th}$  element of the centered and normalized sequences  $\bar{a}_c[n_i]$ ,  $\bar{\phi}_c[n_i]$ , and  $\bar{f}_c[n_i]$  are calculated using [76]

$$\bar{a}_c[n_i] = \frac{a[n_i] - \mu_a}{\max_{1 \leq j \leq N_x} (a[n_j])}, \quad (3.14)$$

$$\bar{\phi}_c[n_i] = \frac{\phi[n_i] - \mu_\phi}{\max_{1 \leq j \leq N_x} (\phi[n_j])}, \quad (3.15)$$

$$\bar{f}_c[n_i] = \frac{f[n_i] - \mu_f}{\max_{1 \leq j \leq N_x} (f[n_j])}, \quad (3.16)$$

where  $1 \leq i \leq N_x$  and  $N_x$  is the total number of elements in  $x_{IQ}[n]$ .

The resultant  $\bar{a}_c[n_i]$ ,  $\bar{\phi}_c[n_i]$ , and  $\bar{f}_c[n_i]$  sequences are divided into  $N_R$  specified regions prior to calculating the desired statistics of standard deviation  $\sigma$ , variance  $\sigma^2$ , skewness  $\gamma$ , and/or kurtosis  $\kappa$  for the signal attribute sequences. Additionally, the statistics can be calculated over the entire signal response (union of all subregion samples). The final *Composite Fingerprint* sequence for  $x_{IQ}[n]$  is formed by concatenating all subregions statistics, and the entire region statistics if generated. This is illustrated in Fig. 3.11 which shows an abstract representation of RF-DNA fingerprint generation using an arbitrary feature sequence [103].

### 3.7 Region of Interest Selection

When processed according to Sect. 3.5, the resultant sequences represent the emission data across an entire LLP scan. Previous efforts that targeted URE responses were based on experiments where the researcher had precise control of the devices being analyzed [10, 11]. As previously discussed, the PLC scan includes not only the logic operations explicitly defined by the LLP, but also includes the

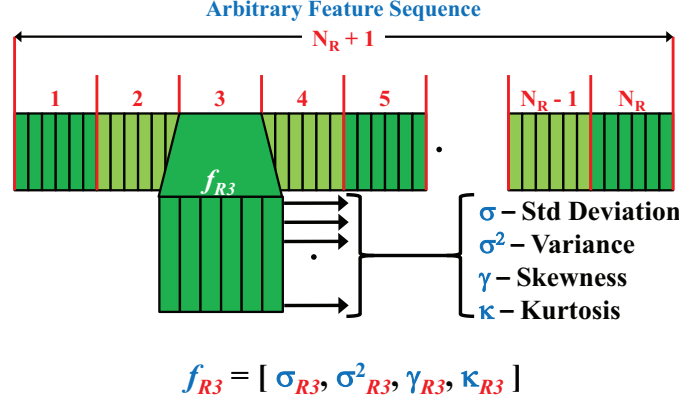


Figure 3.11: Abstract representation of RF-DNA fingerprint formation for an arbitrary sequence divided into  $N_R$  subregions [103]. Standard deviation ( $\sigma$ ), variance ( $\sigma^2$ ), skewness ( $\gamma$ ), and/or kurtosis ( $\kappa$ ) are commonly used as RF-DNA features.

process of evaluating the physical device input values and assigning physical device output values. Additionally, the PLC device also must perform low-level Operating System (OS) functions such as system memory management and interrupt polling. Significant portions of the RF emission signal are not directly attributable to the LLP operations as seen in Fig. 3.12. The signal attributable to the specified LLP operations must be extracted from the entire scan signal to produce a Region Of Interest (ROI). A representative signal collected from an entire scan with the ROI highlighted is pictured in Fig. 3.12. Once the ROI has been identified in a single scan signal, it must be successfully and automatically extracted from the scan signal content. Previous research efforts have involved IRE with clear, definable communication bursts that are clearly separable from the channel noise [34, 39, 76, 97, 102]. Considerable research has been dedicated to detecting and extracting bursts from communication signals [35, 56, 58]. The signals considered for this research effort are URE signals collected from operational PLC equipment, which have a more continuous broadcast model as opposed to the burst broadcast model of communication IRE devices. Additionally, the structure in the TD and SD for URE emissions is not specified or engineered to be collected and processed and are significantly different in

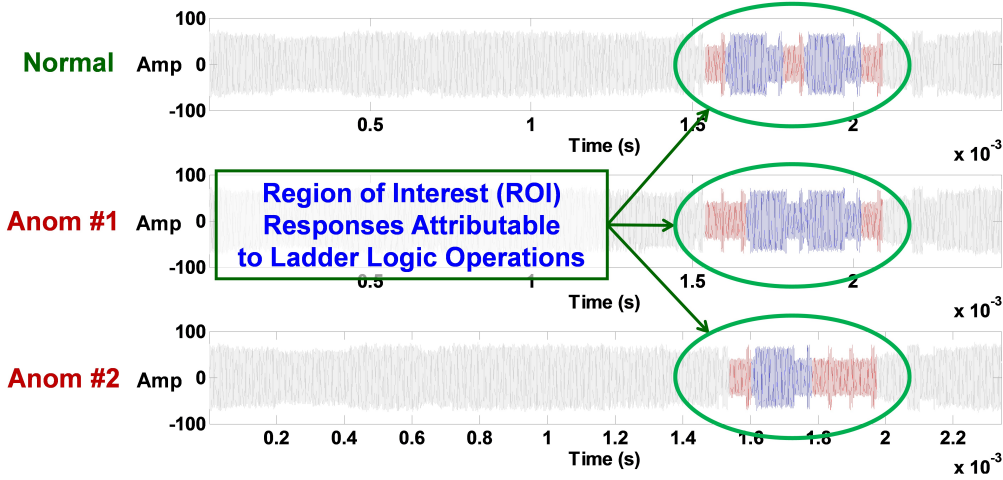


Figure 3.12: Representative TD collected sequences from a PLC device operating under *Norm* and *Anom* conditions as indicated. The highlighted ROI regions represent the response of one full LLP scan.

both domains for different semiconductor devices. These attributes of URE signals provide a unique challenge when extracting the ROI for use in hardware or software anomaly detection.

A correlation-based approach is used in this research in extracting the ROI. Each implemented LLP begins with an *alignment reference* comprised of the  $\{MOV, SQR\}$  LLP operation sequence previously used for probe placement. The  $\{MOV, SQR\}$  sequence is used to detect the beginning of the ROI, containing operation attributable signal content. Each LLP used in this research concludes with either a *MOV* or *SQR* operation, designating the termination of the operation attributable signal content. It is important to make a distinction to the use of LLP operations to detect ROIs and PLC outputs to trigger the collection. Because outputs values are assigned *after* the logical operations are performed, the physical trigger used to initiate the collection of emissions is not aligned to the operation attributable signal content. Additionally, unpredictable operations performed by the PLC MCU preclude the use of a static alignment method.

The following steps are performed on each collected, stored, and post-collection processed signal  $x_C[n]$ . The signal resulting from collections against the  $\{MOV, SQR\}$  LLP,  $x_{AS}[n]$  is referred to as the *alignment start reference*. The alignment reference signal consists only of signal content attributable to the  $\{MOV, SQR\}$  operations, extracted from a representative collected signal prior to the alignment process. The signal resulting from collections against either a  $\{SQR, MOV\}$  LLP (for  $N_{OP}=5$ ) or  $\{SQR\}$  LLP (for  $N_{OP}=10$ ),  $x_{AE}[n]$  is referred to as the *alignment end reference*. The alignment reference and conclusion reference are collected from the same DUT as the sequences that are the source of the ROIs. The correlation process is identical to the correlation process (3.3) used in the probe alignment process discussed in Sect. 3.4.3. The goal, in this case, is to provide a means of not only extracting the ROI from the burst, but also to ensure the operation attributable content of the ROIs are not corrupted by non-operation attributable signal content. In addition to the non-attributable signal content exhibited in Fig. 3.12, the PLC DUT also performs OS and system maintenance functions that may occur between the execution of the LLP operations. *pristine* ROIs are those containing only operation attributable signal content while *corrupted* ROI contain non-attributable content.

The ROIs are extracted and declared pristine or corrupted for a single collected sequence  $x_C[n]$  and alignment reference sequences  $x_{AS}[n]$  and  $x_{AE}[n]$  according to the following:

1. Consider collected sequence  $x_C[n]=\{x_C[n_i]\}$ ,  $i=1, 1, \dots, N_C$  and two alignment reference sequences denoted by  $x_{AS}[n]=\{x_{AS}[n_i]\}$ ,  $i=1, 2, \dots, N_{AS}$ , and  $x_{AE}[n]=\{x_{AE}[n_i]\}$ ,  $i=1, 2, \dots, N_{AE}$ , with all based on collections from the the same DUT.
2. The  $x_C[n]$ ,  $x_{AS}[n]$ , and  $x_{AE}[n]$  sequences are all collected and post-collection processed using identical methods, i.e., filtering, down-sampling, and sequence transformation.

3. Two alignment signals are used:
  - 1)  $x_{A1}[n]=\{x_{AS}[n_1], x_{AS}[n_2], \dots, x_{AS}[n_{N_{ASSamp}}]\}$  and
  - 2)  $x_{A2}[n]=\{x_{AE}[n_{AESamp}], x_{AE}[n_{2-1}], \dots, x_{AE}[n_1]\}$ .
4. The sequence  $x_C[n]$  is divided into two sequences:
  - 1)  $x_{C1}[n]=\{x_C[n_1], x_C[n_2], \dots, x_C[n_{N_{CSamp}}]\}$  and
  - 2)  $x_{C2}[n]=\{x_C[n_{CSamp}], x_C[n_{(2-1)}], \dots, x_C[n_1]\}$ .
5. Cross correlation sequence  $C_{C1,A1}[k]$  is calculated using (3.3) with the  $x_{C1}[n]$  and  $x_{A1}[n]$  sequences as inputs. The value  $\max(C_{C1,A1}[k])=C_{C1,A1}[k_{i_{Max1}}]$  and index for the maximum value  $i_{Max1}$  are found and stored. The value  $i_{Start}=i_{Max1}$  represents the estimated sample number for the ROI *start*.
6. Cross correlation sequence  $C_{C2,A2}[k]$  is calculated using (3.3) with the  $x_{C2}[n]$  and  $x_{A2}[n]$  sequences as inputs. The value  $\max(C_{C2,A2}[k])=C_{C2,A2}[k_{i_{Max2}}]$  and index for the maximum value  $i_{Max2}$  are found and stored. The value  $i_{Max2}$  represents the estimated number of samples from the end of signal  $x_C[n]$  to the *end* of the ROI. The estimated end of the ROI is  $i_{end}=N_{CSamp} - i_{Max2}$  samples from the beginning of the signal  $x_C[n]$ .
7. For each signal  $x_C[n]$  three criteria are used to select the ROIs:
  - 1) Maximum correlation value for ROI start  $C_{MS}=\max(C_{C1,A1}[k])$
  - 2) Maximum correlation value for ROI end  $C_{ME}=\max(C_{C2,A2}[k])$
  - 3) Estimated length in samples of the ROI  $N_{ROIEst}=i_{end} - i_{Start}$ .

The preceding steps are repeated for all  $N_B$  *potential* sequences

$P_{XC}[n]=\{x_{C1}[n], x_{C2}[n], \dots, x_{C1}[n]\}$  to generate sets of criteria values associated with the signals. Potential sequences are those that are still considered as candidates for contributing a non-corrupted ROI. Let  $C_{MS}[n]=\{C_{MS}[n_1], C_{MS}[n_2], \dots, C_{MS}[n_{N_B}]\}$  be the set of maximum correlation values for the ROI start such that  $C_{MS}[n_k]$  is the maximum correlation start value for the collected sequence  $x_{C_k}[n]$ , Similarly, let  $C_{ME}[n]=\{C_{ME}[n_1], C_{ME}[n_2], \dots, C_{ME}[n_{N_B}]\}$ , be the set of maximum correlation values for the ROI end generated from the  $N_B$  collected sequences and



$N_{ROIest}[n]=\{N_{ROIest}[n_1], N_{ROIest}[n_2], ..., N_{ROIest}[n_{N_B}]\}$  be the set of estimated ROI sample length for the collected sequences. Once the criteria have been calculated for all signals considered, the following steps are used to assign a *rank* to the signals so they can be sorted in order of priority: from those most *pristine* to those most *corrupted*. The criteria are used to remove sequences from the list  $P_{XC}[n]$  based on evaluation of the criteria for the sequences.

The first step in extracting sequences that are not corrupted by non-attributable content involves removing sequences based on estimated ROI length  $N_{ROIest}[n]$ . Initially, all collected sequences are considered equal and kept in a set of potential sequences  $P_{XC}[n]=\{x_{C_1}[n], x_{C_2}[n], ..., x_{C_{N_B}}[n]\}$ . For each collected sequence  $x_{C_k}[n], 1 \leq k \leq N_B$  the estimated ROI length is compared to an established threshold. It is assumed that the ROIs from sequences corrupted by the non-operation attributable content will be longer, in samples, than those that do not contain the extra content and sequences with an estimated ROI length exceeding the established threshold are removed from the potential sequence list  $P_{XC}[n]$ . The threshold is established based on the mean and standard deviation values for the estimated ROI length. Consider the mean  $\mu_{ROIest}$  and standard deviation  $\sigma_{ROIest}$  values for the estimated ROI sample length set  $N_{ROIest}[n]$ . A sequence  $x_{C_k}[n]$  is removed from the set of potential sequences  $P_{XC}[n]$  if the estimated ROI length exceeds the threshold  $N_{ROIest}[n_k] > \mu_{ROIest} + 0.3\sigma_{ROIest}$ . This threshold was empirically chosen to offer an acceptable balance of removing sequences with potentially corrupted ROIs and keeping an adequate number of sequences for evaluation of the CBAD process.

Following removal of sequences that exceed the threshold  $N_{ROIest}[n] > \mu_{ROIest} + 0.3\sigma_{ROIest}$ , the remaining sequences in the list are assigned a rank  $r_x[n]$  based on the maximum start and end correlation values  $C_{MS}$  and  $C_{ME}$ . A sequence,  $x_{C_k}[n]$  in the list  $P_{XC}$  is assigned rank  $r_x[n_k]=\mu_{MS,ME}[n_k]$ . The value  $\mu_{MS,ME}[n_k]$  is the mean of the 2-element set  $\{C_{MS}[n_k], C_{ME}[n_k]\}$ , the maximum correlation values for the estimated start and end of the ROI for sequence  $x_{C_k}[n]$ . The

remaining sequences in the potential sequence set  $P_{XC}[n]$  are restructured in descending order such that  $P_{XC}[n_1]$  is the sequence with the maximum value for  $\mu_{(MS,ME)}[n]$ . Sequences considered for evaluation are taken from the sorted set  $P_{XC}[n]$ . For a desired number of selected sequences  $N_{Sel}$ , the set of ordered sequences  $P_{Sel}[n]=\{P_{XC}[n_1], P_{XC}[n_2], \dots, P_{XC}[n_{N_{Sel}}], \}$  is used for evaluation of the process.

Once the final list of  $N_{Sel}$  selected sequences  $P_{Sel}[n]=\{P_{Sel}[n_1], P_{Sel}[n_2], \dots, P_{Sel}[n_{N_{Sel}}]\}$  has been established, the ROIs must be extracted. The ROIs are extracted based on the sample index  $i_{Start}$  where the maximum start correlation value was found. The ROI length  $N_{ROI}$  is established based on empirically observed ROI length for a representative sequence. For a sequence  $x_C[n]=P_{Sel}[n_k]=\{x_C[n_1], x_C[n_2], \dots, x_C[n_{N_s}]\}$  with a maximum start correlation index  $i_{Max}$  the ROI  $x_{ROI}[n]=\{x_C[n_{i_{Max}}], x_C[n_{i_{Max}+1}], \dots, x_C[n_{i_{Max}+N_{ROI}-1}]\}$ .

### 3.8 CBAD Processing

The CBAD overview was presented in Sect. 3.3 and more details are provided here on key processing steps. The first step involved collecting RF emission sequences from each DUT operating under *Norm*, *Anom #1*, and *Anom #2* operating conditions. For CBAD evaluation under this research, the collections were performed for  $N_D=10$  PLC devices executing both the  $N_{OP}=5$  (Sect. 3.2.1) and  $N_{OP}=10$  (Sect. 3.2.1) LLPs; the actual number of LLP operations is not significant for the remaining discussion in this section. The sequences are collected and stored as outlined in Sect. 3.4 and post-collection processed as outlined in Sect. 3.5.

The CBAD process is presented once, but is repeated for each device and at each desired *SNR* independently. The *Normal* reference sequence is only generated once and is not scaled for different *SNR* values.

*3.8.1 Testing and Training Set Generation.* The ROIs are extracted from the collected and processed bursts as outlined in Sect. 3.7. The number of ROIs

selected varied from  $N_B=1$  collected ROI selected for an initial proof of concept to  $N_B=1000$  ROIs selected for the final results. The number of collected sequence ROIs is not significant to the discussion of the process. The ROIs are separated into two independent “Training” ( $x_{Tng}[n]$ ) and “Testing” ( $x_{Tst}[n]$ ) data sets; the “Training” and “Testing” distinction adopted here for consistency with terminology used in the pattern recognition community [22]. The training sequences were selected based on an *interleaved* pattern. Assume a total of  $N_B=1000$  ROIs are in the set  $x_C[n]$  and  $\%Tng=5\%$  are selected as training sequences; a total of  $N_{Tng}=50$  are used as training sequences. In any situation where the value for  $\%Tng$  and  $N_B$  do not result in an integer number, the number is rounded down to the nearest integer. Using an interleaved selection pattern, the training set  $x_{Tng}[n]$  is constructed from sequences in  $x_C[n]$  by taking every other sequence (e.g., the odd numbered ones) out of  $x_C[n]$ . The remaining  $N_{Tst}=N_B-N_{Tng}$  sequences in  $x_C[n]$  (e.g., the even numbered ones) are placed in the testing set  $x_{Tst}[n]$ .

While the CBAD process is trained only on the *Normal* sequences, the training and testing selection process is performed on the *Normal* and *Anomalous* sets such that all testing sets have the same number of sequences. For clarity, let the normal test set be  $x_{TstN}[n]$ , the anomalous condition#1 test set be  $x_{TstA1}[n]$  and the anomalous condition#2 test set be  $x_{TstA2}[n]$ . The normal condition training set is  $x_{Tng}[n]$  since there are no training sets for the anomalous condition.

For each desired  $SNR$ , the  $N_{Tst}$  *Norm*, *Anom #1* and *Anom #2* testing sequences are each added to  $N_{Nr}$  AWGN realizations for a total of  $N_{TestRlz}=N_{Tst} \times N_{Nr}$  sequences used as testing sequences. For the purpose of this CBAD process discussion, the focus is on a single  $SNR$ , device, operating condition permutation. The steps in the CBAD process are implemented identically irrespective of what input sequences are used.

*3.8.2 Reference Sequence  $x_R[n]$  Generation.* The next step is to generate the Normal Reference sequence  $x_R[n]$  in Fig. 3.3 using the  $N_{Tng}$  *normal* sequences contained in the “Training” data set  $x_{Tng}[n]$ . Recall, the training set is composed entirely of sequences for the normal condition LLP *Norm*. As functionally denoted in (3.17), the CBAD process accepts two inputs, a *Reference* sequence  $X_R[n]$  and an unknown *Collected* sequence  $x_C[n]$ , and outputs a single real-valued output test statistic ( $z_V$ ) or

$$z_V = CBAD(x_N[n], x_C[n]) . \quad (3.17)$$

The CBAD function is first used with input “Training” sequences  $x_{Tng}[n]$  to generate the desired *Normal* operating sequence  $x_N[n]$ . After setting the reference  $x_R[n]=x_N[n]$  as illustrated in Fig. 3.3, the CBAD function is then used to generate the collection of “Testing” verification test statistics  $z_V$ . The reference sequence  $x_R[n]=x_N[n]$  sequence is generated as follows:

1. Construct a set of  $N_{Pot}=N_{Tng} + 1$  *potential* reference sequences  $x_{Pot}[n]$  consisting of the  $N_{Tng}$  “Training” sequences  $x_{Tng}[n]$  and the sequence  $\bar{X}_{Pot}[n]$  calculated as an average of  $N_{Tng}$  sequences. The final normal reference sequence  $x_N[n]$  is selected from the set of potential sequences  $x_{Pot}[n]$ .

$$\bar{z}_{V_i} = \frac{\sum_{j=1}^{N_{Pot}-1} CBAD(x_N[n] = x_{Pot_i}[n], x_C[n] = x_{Pot_j}[n])}{N_{Pot} - 1} \quad (3.18)$$

$$: i = 1, 2, \dots, N_{Pot}; j = 1, 2, \dots, N_{Pot}; i \neq j .$$

2. Consider the set of average statistic values resulting from the process in Step 2  $\bar{z}_V[n]$ . The selected reference sequence is the potential reference sequence that, when used as a reference sequence, yields the minimum average verification statistic

$$x_N[n] = x_{Pot_i}[n] \ni \bar{z}_V[n_i] = \min(\bar{z}_V[n_1], \bar{z}_V[n_2], \dots, \bar{z}_V[n_{N_{Pot}}]) . \quad (3.19)$$

Once the *Norm* reference is selected, it is used as the reference sequence for the remainder of CBAD processing.

*3.8.3 Test Statistic  $z_V$  Generation.* The cross-correlation sequence  $C_{NC}[k]$  is generated for each test sequence using the selected  $x_R[n]$  reference sequence and test Sequence  $x_{Tst}[n]$  to be verified. This part of the process is completed for every sequence in the test sequence set, but is presented for a single sequence to clearly outline the process. The resultant  $C_{NC}[k]$  is then subtracted from the auto-correlation sequence  $C_{NN}[k]$  to generate the correlation difference sequence as  $C_{\Delta}[k]=C_{NN}[k]-C_{NC}[k]$ .

For a reference sequence  $x_R[n]$  and test sequence  $x_{Tst}[n]$  of equal size  $N_s$ , the correlation difference sequence  $C_{\Delta}[k]$  consists of  $N_{CorrSamp}=2N_s-1$  samples. In order to support the binary decision of declaring the sequence *anomalous* or *normal* the correlation difference sequence  $C_{\Delta}[k]$  is used to generate a single statistic value  $z_V$ . The verification test statistic  $z_V$  is calculated using a pre-selected difference function ( $f_{\Delta}$ ) and  $C_{\Delta}[k]$  as  $z_V=f_{\Delta}(C_{\Delta}[k])$ . For all results presented here, the difference function is implemented as  $f_{\Delta}=|C_{\Delta}[k]|$ , i.e., a simple 2-norm magnitude operation.

Once the CBAD statistics have been generated, the input sequences  $x_{Tst}[n]$ ,  $x_{Tng}[n]$ , and  $x_R[n]$  are no longer used.

*3.8.4 Verification Threshold Determination.* The next step in the CBAD process is to establish the desired verification threshold  $t_V$ . There are three CBAD statistic sets resulting from the previous step in the CBAD process: 1) the statistic set for the *Norm* operating condition  $z_{VN}[n]$ , 2) the statistic set for the *Anom* #1 operating condition  $z_{VA1}[n]$ , and 3) the statistic set for the *Anom* #2 operating condition  $z_{VA2}[n]$ . Recall, each set is the same size and contains  $N_{Tst}$  statistics.

The interleaved selection of *testing* and *training* sequence sets was repeated for the statistic set  $z_{VN}[n]$ . The threshold value  $t_V$  was established using the collection

of *training* verification test statistics  $z_{VTng}[n]$  and corresponding Probability Mass Function (PMF)  $P_{Z_V}(z_{VTng})$ . For a desired  $FADR_D$  performance the threshold  $t_V$  was set such that the following is satisfied,

$$P[Z_{PTng} > t_V] = FADR_D , \quad (3.20)$$

where  $Z_{PTng}$  is the random variable with a distribution defined by the observed PMF  $P_{Z_V}(z_{VTng})$  for the set of test statistics  $z_{VTng}[n]$ .

**3.8.5 Anomalous vs. Normal Declaration.** Declaring input sequence  $x_{Tst}[n]$  as being *Norm* or *Anom* was based on test statistics  $z_{VTst}$  derived from  $x_{Tst}[n]$ . The final declaration is made using a simple comparison of input test statistic  $z_{VTst}$  with the established Verification Threshold  $t_V$  according to

$$\begin{aligned} z_{VTst} < t_V &\rightarrow x_{Tst}[n] : \text{Normal} \\ z_{VTst} > t_V &\rightarrow x_{Tst}[n] : \text{Anomalous} . \end{aligned} \quad (3.21)$$

### 3.9 LLP Operation-by-Operation Processing

The CBAD process in Sect. 3.8 operates on entire input sequences and calculates a single CBAD statistic for the entire waveform. An alternate method for calculating CBAD statistics is to use multiple *reference* sequences consisting of stored sequences for each LLP operation in the *Norm* operating condition. The *anomalous* LLPs used to generate the collected emissions differ in either  $N_{OP}=1$  (*Anom #2*) or  $N_{OP}=2$  operations (*Anom #1*) from the *Norm* operating condition LLP *Norm*. The length, in samples, for the altered LLP operation dictates the number of samples that are different in the anomalous emissions. This step in the research effort focused on leveraging knowledge of the normal operating sequence using  $N_{OP}=10$  unique reference signals to evaluate each LLP operating region for anomalous (different from the normal) behavior. Figure 3.13 shows the  $|H[x[n]]|$  emission sequence

with the  $N_{OP}=10$  operations clearly depicted. The change in emissions due to a

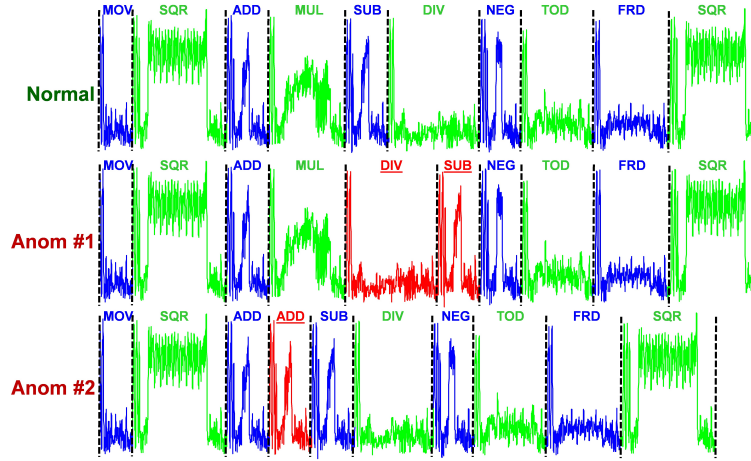


Figure 3.13: Emission sequences with  $N_{OP}=10$  LLP operations being clearly attributable to specific subregions. Operations highlighted in red represent changes that were made to the *Norm* LLP to simulate anomalous operating conditions in the *Anom #1* and *Anom #2* LLPs.

single altered operation may not be enough to surpass the detection threshold  $t_V$ . Therefore, an Operation-by-Operation CBAD process is employed where each operation is weighted equally when making the decision to declare anomalous or normal regardless of the actual ratio of total samples the operation-attributable signal occupies.

The operation-by-operation implementation of the CBAD detection process computes multiple CBAD statistics arranged in a sequence or *CBAD statistics vector*  $\langle z_{V_1}, z_{V_2}, \dots, z_{V_{N_{OP}}} \rangle$  where  $N_{OP}$  is the number of LLP operations in the *normal* operating condition program. The CBAD statistics are calculated for each of the *Norm* LLP operation regions seen Fig. 3.13. Each delineated operation region has a reference emission used to calculate the CBAD statistic for that operation region. The  $N_{OP}$  *Norm* operations clearly align with the operation-by-operation regions while the *Anom #1* and *Anom #2* operations do not.

Figure 3.14 illustrates the flow of the Operation-by-Operation CBAD process showing parallel CBAD statistic calculations used to generate the  $N_{OP}$  CBAD statistics vector. The function  $f_Z(\cdot)$  used to reduce the CBAD statistics vector  $\langle z_{V_1}, z_{V_2}, \dots, z_{V_{N_{OP}}} \rangle$  is the 2-norm magnitude function  $|\langle z_{V_1}, z_{V_2}, \dots, z_{V_{N_{OP}}} \rangle|$ . The end result is still a single CBAD statistic used to declare the operating condition *normal* or *anomalous* based on a threshold  $t_V$ .

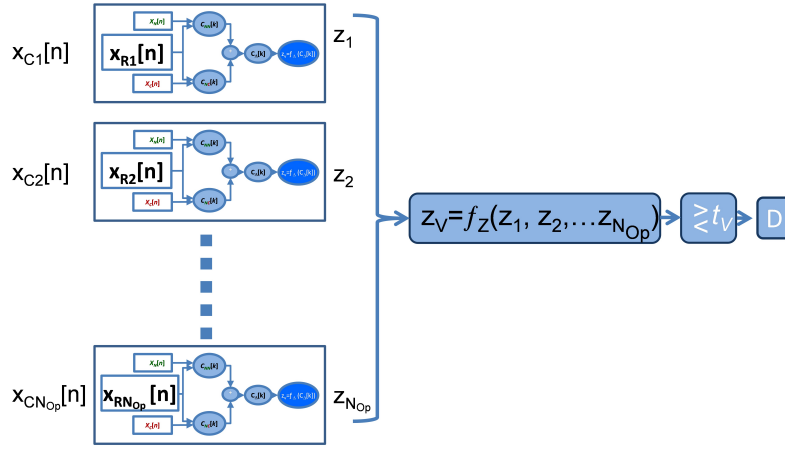


Figure 3.14: Parallel CBAD processing used to perform LLP operation-by-operation correlation. The branch test statistics ( $z_i$ ) are used to form a composite CBAD test statistic vector for final verification assessment, with a 2-norm magnitude used to make the final *Norm* or *Anom* declaration.

### 3.10 Performance Evaluation

Verification performance was evaluated for this research using 1) True Anomaly Detection Rate (TADR) vs. SNR performance curves, and 2) traditional Receiver Operating Characteristic (ROC) curves generated by plotting False Anomaly Detection Rate (FADR) vs. TADR based on discrete PMFs formed using selected test statistics.

**3.10.1 Performance Curves.** The TADR vs. SNR performance curve is generated by plotting the TADR for each SNR considered. Before the TADR values



can be calculated, a threshold  $t_V$  must be established to determine what statistic values result in an *anomalous* declaration and what statistic values result in a *normal* declaration. Each SNR value considered has a unique threshold value  $t_V$  calculated for use with sequences at that SNR. The threshold  $t_V$  is calculated at each SNR value considered to provide  $FADR=10.0\%$ . The arbitrary Benchmark  $TADR_B=90.0\%$  is used to determine the SNR value used for ROC curve generation.

*3.10.2 CBAD Statistical PMFs.* The experimental PMF derived from the calculated CBAD statistics is used to generate the ROC curves. The PMFs are experimentally determined and are generated in keeping with accepted random process and signals methods [51]. It is also used to provide a qualitative measure of separation between CBAD statistic values associated with the different operating conditions or hardware devices. The PMFs are experimentally generated and depend on a selection of a specific SNR value. The selected SNR value is the lowest valued SNR that satisfies the benchmark  $TADR_B=90.0\%$  as specified in the previous section.

*3.10.3 ROC Curve Assessment.* The ROC curves are generated in keeping with accepted biometric standards and methods [48]. The ROC curve is generated using the results of the experimental PMF calculations. A ROC curve consists of data plotted for FADR vs. TADR and provides a means of comparing detectors based on the Equal Error Rate (EER). The EER is the point at which the two errors associated with verification (FADR and False Normal Verification Rate (FNVR)) are equal in keeping with accepted biometric verification standards and practices. [48]. The arbitrary benchmark for the EER is  $EER_B=10.0\%$ . This goal is determined by the relationship of the FNVR and the performance benchmark of  $TADR_B=90.0\%$ :  $FNVR=1 - TADR$ .

ROC curves are generated by varying the threshold  $t_V$  and calculating the FADR and TADR values for each variation in threshold. Consider a set of *normal*

CBAD statistics  $z_N[n]$  with  $N_{ZN}$  elements and a set of *anomalous* CBAD statistics  $z_A[n]$  with  $N_{ZA}$  elements. Let  $t_V[n]$  be the set of  $N_V$  threshold values arranged in ascending order such that  $t_V[n_i] < t_V[n_j]$ ,  $1 \leq i < j \leq N_V$ ,  $i \neq j$ . Considering the union of *Norm*  $z_N[n]$  and *Anom*  $z_A[n]$  CBAD statistics,

$$z_U = \{z_N[n_1], z_N[n_2], \dots, z_N[n_{N_{ZN}}], z_A[n_1], z_A[n_2], \dots, z_A[n_{N_{ZN}}]\} , \quad (3.22)$$

Let  $t_V R[n]$  be the set of threshold values used to generate the ROC curve. The number of threshold values in the set  $t_V[n]$  is dictated by the desired ROC resolution. For this research, a total of  $N_V=100$  threshold values were sufficient for ROC curve analysis. The set of  $N_V=100$  threshold values  $t_V[n]$  used to generate the ROC curve is based on the values in  $z_U$  where  $t_V[n_1]$  is set equal to the minimum value of  $z_U$ ,

$$t_V[n_1] = \min\{z_U\} , \quad (3.23)$$

and the remaining elements are defined by

$$t_V[n_i] = t_V[n_{(i-1)}] + \frac{(\max\{z_U\} - \min\{z_U\})}{N_V - 1} \quad (3.24)$$

$$: i = 2, 3, \dots, N_V .$$

### 3.11 GRLVQI Processing

A majority of the initial research activity focused on *software anomaly detection*—discriminating between various *operating conditions* to detect malfunctioning or malicious software, firmware, etc. However, an important parallel avenue of research developed to support *hardware device discrimination*—discriminating between various *hardware components* to detect malfunctioning or counterfeit, trojan, etc., Integrated Circuits (IC).

It was determined that the proposed verification-based anomaly detection process was well-suited for the *hardware device discrimination* task and initial proof-of-

concept demonstration was conducted using the GRLVQI process developed in [76]; the process was not modified under this effort so the minimal details are presented here. The GRLVQI process is inherently signal agnostic and can accept any type of sequence as input. For demonstrations here, two specific types of input sequences were considered: 1) TD feature sequences and 2) Correlation Domain (CD) feature sequences. The TD feature sequences  $f_{TD}[n]$  were generated using the RF-DNA process in Sect. 3.6.2 with  $N_R=12$  subregions plus the total response, all three instantaneous features, and all four statistics, for a total of  $N_F=156$  features in each *Composite Fingerprint* sequence.

To demonstrate *hardware device discrimination*, a single LLP was used to generate sequences for multiple PLC devices with goal of maintaining constant operating conditions to ensure discrimination was based on device hardware. The  $N_{OP}=10$  LLP for *Normal* operating conditions was used to generate the RF-DNA  $f_{TD}[n]$  feature sequence for use in the hardware discrimination portion of the research.

In addition to TD feature sequences, the GRLVQI method of verification was evaluated using CD feature sequences  $f_{CD}[n]$  that were generated using the Operation-by-Operation CBAD process described in Sect. 3.9. Instead of creating a single CBAD statistic  $z_V$ , a collection of CBAD statistics  $\{z_{1V}, z_{2V}, \dots, z_{N_{10}V}\}$  were generated using  $N_{Op}=10$  LLPs. These CBAD statistic sequences  $f_{CD}[n]=\{z_{1V}, z_{2V}, \dots, z_{N_{10}V}\}$  were used as input sequences for GRLVQI verification performance assessment.

Performance of the GRLVQI process was evaluated for both TD  $f_{TD}[n]$  and CD  $f_{CD}[n]$  feature sequences using ROC curves and benchmark performance criteria presented in Sect. 3.10.3.

## 4. Results

This chapter provides research results for *software anomaly detection* and *hardware component discrimination* based on the methodology presented in Chapter 3. Section 4.1 first introduces the various Programmable Logic Controller (PLC) response sequences used for generating results and assessing performance. Results for *software anomaly detection* via verification using the Correlation Based Anomaly Detection (CBAD) process are presented in Section 4.3 for Time Domain (TD) PLC input sequences, Section 4.4 for statistical Radio Frequency Distinct Native Attributes (RF-DNA) input sequences, and Section 4.5 for Hilbert transformed input sequences. The chapter concludes with Section 4.6 which demonstrates *hardware component discrimination* via verification using a Generalized Relevance Learning Vector Quantization-Improved (GRLVQI) classification process with both TD and Correlation Domain (CD) statistical features as inputs.

### 4.1 PLC Response Sequences

The experimental methodology described in Chapter 3 is first used to demonstrate applicability of the CBAD process for reliably detecting anomalous software operating conditions. This is done using the specific ladder logic programs described in Section 3.2 and collected signals described in Section 3.7.

Results for this research are based on unintentional TD emissions collected from Allen Bradley SLC-500 PLC Central Processing Unit (CPU) modules. These emissions are sampled, stored, and post-collection processed using the methodology and configurations specified in Chapter 3. The emissions are collected from selected PLC devices executing  $N_{OP}=5$  and  $N_{OP}=10$  Ladder Logic Program (LLP) operations. The term *burst* is introduced as a general term to refer to a collected, sampled, and post-collection processed emission. Specific details of the LLPs used to generate PLC emissions are provided in Section 3.2.

There are four types of PLC response sequences generated from the experimentally collected TD emissions and each was used in some manner to evaluate CBAD and/or GRLVQI processes. The four sequences included: 1) the TD magnitude response sequences  $|x[n]|$ , 2) the magnitude of Hilbert transformed TD response sequence  $|H[x[n]]|$ , 3) the statistical RF-DNA TD response sequence  $f_{TD}[n]$  and 4) the CD response sequence  $f_{CD}[n]$ . All four types of sequences served as input sequences for evaluation and were derived from PLC bursts as described in Chapter 3.

#### 4.2 Performance Evaluation Criteria

Three evaluation criteria were used to assess *software anomaly detection* performance relative to an arbitrary Benchmark (B) defined by 1) Signal-to-Noise Ratio ( $SNR_B$ ), 2) True Anomaly Detection Rate ( $TADR_B$ ), and 3) Equal Error Rate ( $EER_B$ ). The following steps were used to derive resultant performance metrics relative to the established benchmark:

1. Generate verification results for varying  $SNR$  using a given anomaly detection method and input sequence type pairing and plot  $SNR$  vs.  $TADR$ .
2. Determine the lowest  $SNR$  at which the plotted  $TADR=TADR_B$ . An arbitrary  $TADR_B \geq 90.0\%$  benchmark was chosen here for assessment. The corresponding  $SNR_B$  at which  $TADR=TADR_B$  is used for Receiver Operating Characteristic (ROC) curve generation.
3. Generate a ROC curve by plotting False Anomaly Detection Rate ( $FADR$ ) vs.  $TADR$  at  $SNR_B$ . The corresponding Equal Error Rate ( $EER$ ) point is determined as the point on the ROC curve at which  $FADR=FNVR=1-TADR$  where  $FADR$  is the False Anomaly Detection Rate. An arbitrary benchmark of  $EER_B \leq 10.0\%$  was chosen here for assessment.

**Performance:** A given anomaly detection method and input sequence pair is deemed inadequate if it does not achieve the arbitrary  $TADR_B \geq 90.0\%$  or  $EER_B \leq 10.0\%$  benchmarks.

### 4.3 Software Anomaly Detection: TD Sequences

The first evaluations of the CBAD process were conducted using TD magnitude sequences  $|x[n]|$  derived from sampled, post-collection processed PLC emissions as described in Section 3.5; the input TD sequences are simply transformed by taking the magnitude of each sample ( $|x[n]|$ ), with no Hilbert transform applied. Two methods were initially used to evaluate the plausibility of using CBAD processing to detect changes in the PLC operating condition: 1)  $N_B=1$  TD magnitude sequence  $|x[n]|$  combined with  $N_{Nr}=200$  Additive White Gaussian Noise (AWGN) realizations to achieve the desired Analysis Signal-to-Noise Ratio ( $SNR_A$ ), and 2)  $N_B=60$  TD magnitude sequences  $|x[n]|$  combined with  $N_{Nr}=10$  AWGN realizations to achieve the desired analysis  $SNR_A$ . For both methods only one PLC device was used to generate  $|x[n]|$  input sequences.

**Notation:** Unless noted otherwise,  $SNR$  is used exclusively to represent  $SNR_A$  throughout the remainder of the document.

**Presentation:** Subsequent use of  $N_{Nr}$  notation refers to the total number of independent, randomly generated AWGN noise realizations  $\{x_{B1}[n], x_{B2}[n], \dots, x_{BNr}[n]\}$  used to power-scale selected sequences to evaluate performance at the desired  $SNR$ .

*4.3.1 Single Device,  $N_B=1$ ,  $N_{Op}=5$ .* The anomaly detection process was initially assessed using a single ( $N_B=1$ ), representative PLC TD magnitude sequence  $|x[n]|$  from the PLC operating under *Norm*, *Anom #1*, and *Anom #2* conditions using  $N_{Op}=5$  operations. For the single response detection, the same burst with varying analysis  $SNR$  was used for both *training* and *testing*. This was done to demonstrate the impact of  $SNR$  variation and noise degradation on CBAD performance without the effects of input signal variation being present. The initial demonstration was performed on a single PLC device denoted as *WQ*. The anomaly

detection process was repeated for  $SNR \in [-30.0, 30.0]$  dB using  $N_{Nr}=200$  AWGN noise realizations per  $SNR$ . This yielded a total of  $N_z=200$  independent CBAD verification statistics ( $z_V$ ) for each operating condition at each  $SNR$  considered.

Figure 4.1 shows anomaly detection  $SNR$  vs.  $TADR$  performance for  $SNR \in [-30.0, 30.0]$  dB. As indicated, the  $TADR_B \geq 90.0\%$  benchmark is achieved for  $SNR \geq -10.0$  dB. Based on these results, anomaly detection ROC performance was evaluated at  $SNR = -10.0$  dB using TD magnitude sequence  $|x[n]|$  and the same conditions as used for Fig. 4.1 results; the PLC operating under *Norm*, *Anom #1*, and *Anom #1* conditions using  $N_{OP}=5$  LLP operations. ROC performance results are presented in Fig. 4.2 and reflect  $EER \leq 3.2\%$  which meets the  $EER_B \leq 10.0\%$  benchmark.

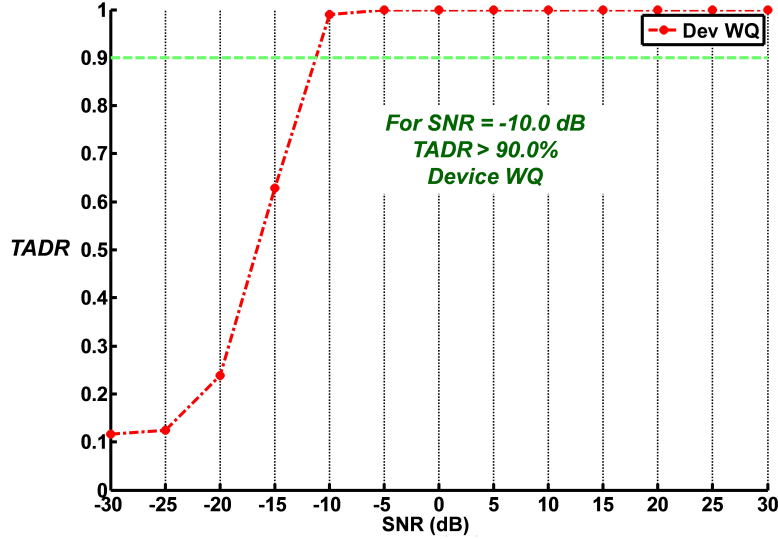


Figure 4.1:  $SNR$  vs.  $TADR$  performance using TD magnitude sequence  $|x[n]|$  for  $N_B=1$  burst with the PLC operating under *Norm*, *Anom #1*, and *Anom #1* conditions using  $N_{OP}=5$  LLP operations. The  $TADR_B > 90.0\%$  benchmark is achieved for  $SNR \geq -10.0$  dB.

**4.3.2 Single Device,  $N_B=60$ ,  $N_{OP}=5$ .** The anomaly detection process performed in Section 4.3.1 was repeated using  $N_B=60$  TD sequences per operating

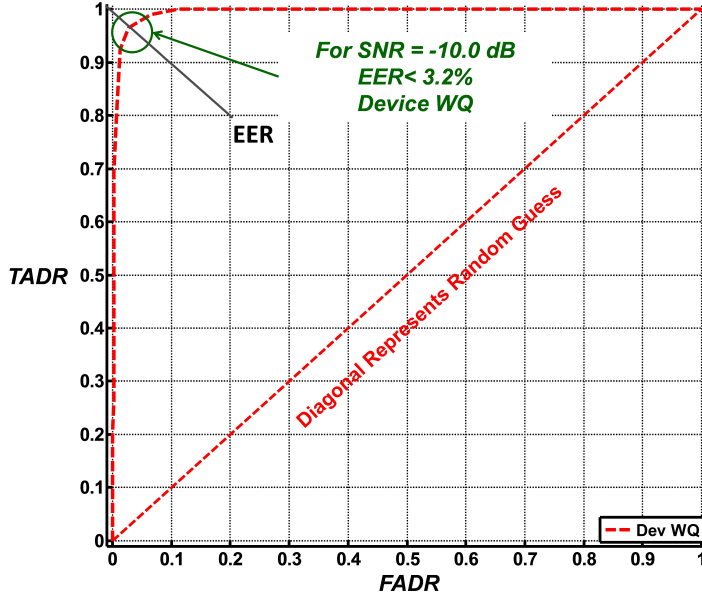


Figure 4.2: Anomaly detection ROC curve for the  $SNR = -10.0$  dB operating point in Fig. 4.1. Results generated using the TD magnitude sequence  $|x[n]|$  with  $N_B=1$  burst and the PLC operating under *Norm*, *Anom #1*, and *Anom #1* conditions using  $N_{OP}=5$  LLP operations. The  $EER_B \leq 10.0\%$  benchmark is achieved.

condition for the *Norm*, *Anom #1*, and *Anom #1*  $N_{OP}=5$  operating conditions. There were  $N_{Tng}=3$  bursts selected as training burst, leaving  $N_{Tst}=57$  bursts per operating condition for CBAD processing evaluation. As in the single response case, the multiple response process was repeated for  $SNR \in [-30.0, 30.0]$  dB and contains representative bursts collected from the *WQ* device. For each  $SNR$  considered, anomaly detection was based on  $N_{Nr}=10$  AWGN noise realizations per  $SNR$ . This yielded a total of  $N_z=570$  test statistics for each operating condition at each  $SNR$  considered.

Figure 4.3 shows  $SNR$  vs.  $TADR$  performance for  $SNR \in [-30.0, 30.0]$  dB. The  $TADR_B \geq 90.0\%$  benchmark is not achieved for any  $SNR$  considered. This is due to variation in the  $N_B=60$  TD waveforms. Each burst represents a unique, collected signal with content that, while attributable to the operations in the LLP, is not identical to the content in the other bursts. The CBAD process is designed to detect variations from the *normal* conditions. The  $N_{Tst}=57$  test input sequences vary



enough from the  $N_{Tng}=3$  training input sequences that even the *Norm* sequences are incorrectly declared anomalous.

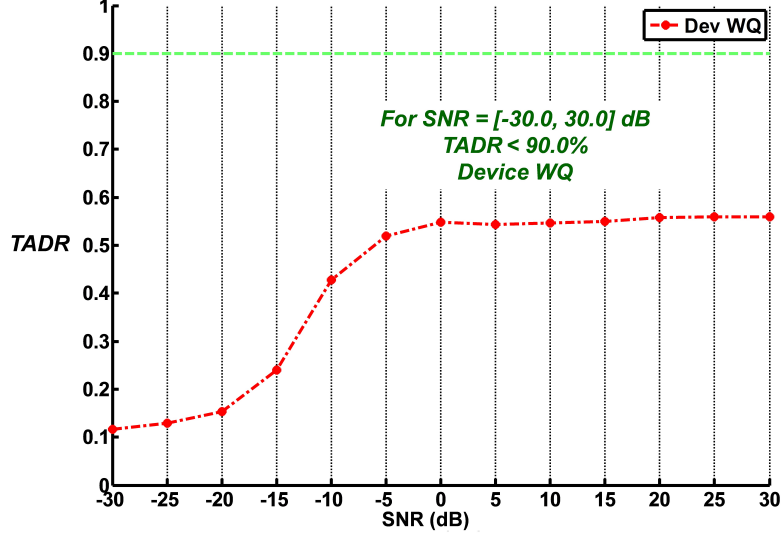


Figure 4.3: *SNR* vs. *TADR* performance using TD magnitude sequence  $|x[n]|$  for  $N_B=60$  bursts with the PLC operating under *Norm*, *Anom* #1, and *Anom* #1 conditions using  $N_{OP}=5$  LLP operations. The  $TADR_B > 90.0\%$  benchmark is not achieved for any  $SNR \in [-30.0, 30.0]$  dB.

Based on results in Fig. 4.3, ROC curve performance was assessed at  $SNR = 30.0$  dB for the multiple response TD waveform bursts. Although *TADR* performance did not achieve the  $TADR_B \geq 90.0\%$  benchmark for any  $SNR$  considered,  $SNR=30.0$  dB yielded the highest *TADR* performance and was chosen to complete ROC analysis. As seen in Fig. 4.4, the  $EER_B \leq 10.0\%$  benchmark is not achieved for  $SNR=30.0$  dB.

Figure 4.5 shows experimentally derived Probability Mass Function (PMF)  $P[Z_V=z_V]$  for the pool of test statistics under *Norm*, *Anom* #1 and *Anom* #2 operating conditions using  $N_B=60$  TD bursts and  $N_{Nr}=10$  AWGN noise realizations scaled to achieve  $SNR=30.0$  dB. Due to variation in collected waveform responses under specified operating conditions, the variance in  $z_V$  here is greater than what was observed for the  $N_B=1$  case. As the PMF response indicate, the *Norm* condition

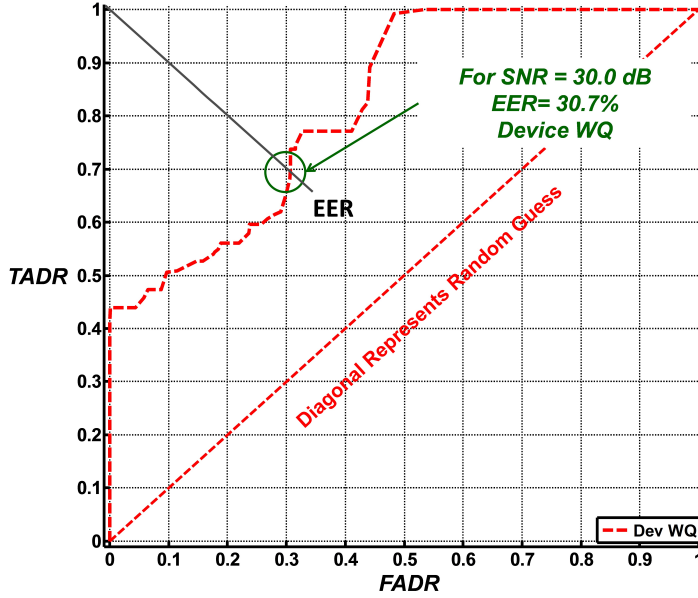


Figure 4.4: Anomaly detection ROC curve for  $SNR=30.0$  dB operating point in Fig. 4.3. Results obtained using TD magnitude sequence  $|x[n]|$  for  $N_B=60$  bursts with the PLC operating under *Norm*, *Anom #1*, and *Anom #1* conditions using  $N_{OP}=5$  LLP operations. The  $EER_B \leq 10.0\%$  benchmark is not achieved.

$z_V$  range significantly overlaps the range of  $z_V$  for both *Anom #1* and *Anom #2* conditions. The  $z_V$  ranges for normal and anomalous operations overlap and are not completely separable for any  $SNR$  considered.

**Performance:** The *Untransformed TD Sequences* were insufficient for reliably detecting anomalous operating conditions and the desired benchmark performance was not achieved using multiple bursts [87,89].

#### 4.4 Software Anomaly Detection: RF-DNA Sequences

Failure of the software anomaly detection process when using multiple collected PLC emissions motivated the need for an alternate representation of anomalous and normal operating conditions. Previous research efforts have found success in classification and verification processes based on using statistical features extracted from collected waveforms [11, 58, 79, 102]. The next step in this research effort was

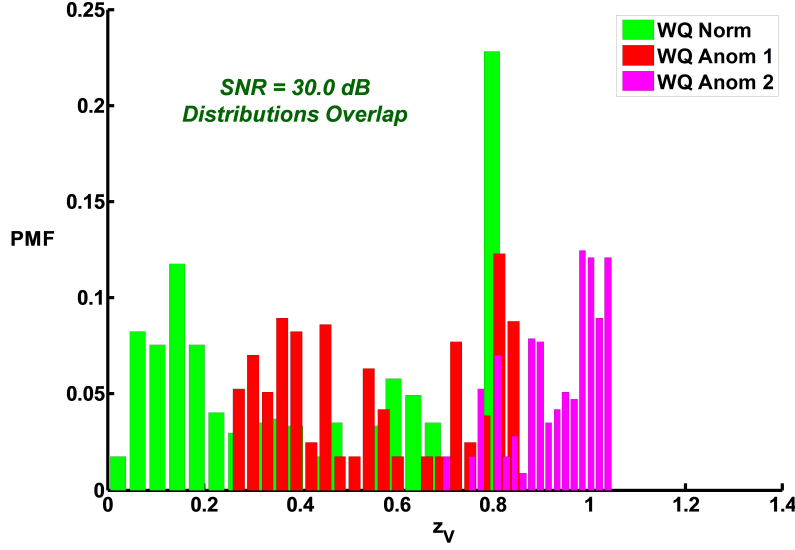


Figure 4.5: Representative PMFs for the PLC  $WQ$  device operating under *Norm*, *Anom #1* and *Anom #2* operating conditions using  $N_B=60$  TD bursts and  $N_{Nr}=10$  AWGN noise realizations scaled to achieve  $SNR=30.0$  dB. There is significant overlap between the *anomalous* PMF  $z_V$  and *normal* PMF  $z_V$ ; perfect anomalous-normal separation and reliable verification is not achievable.

to consider using sequences formed from the statistical features of the waveforms as the input to the anomaly detection process.

As stated in Section 3.3, the anomaly detection process is signal agnostic and can operate on any discrete input sequence. For the feature-based anomaly detection process, the set of input sequences  $\{x_N[n], x_R[n], x_C[n]\}$  are a series of values representing the statistical attributes of a given TD sequence, i.e.,  $\{f_{TDN}[n], f_{RDN}[n], f_{CDN}[n]\}$ , respectively. As outlined in Section 3.6.2, the *Feature Extraction* and *Statistical Fingerprint Generation* processes are used to create a *Composite Fingerprint* based on the collected emission [11, 103]. The Composite Fingerprint reduces the dimensionality of the sequence used in the anomaly detection process. The TD sequences considered for this research are represented by an  $N_D=7500$  dimensional vector, where the dimensionality is a function of the sampling rate  $f_s$  and time length

$T_{WF}$  of the TD emission 4.1.

$$N_D = f_s \times T_{WF} \quad (4.1)$$

The process is graphically depicted in Fig. 3.11 and produces an  $N_D=156$  dimensional vector using  $N_R=12$  sub regions and the total signal,  $N_{Stat}=4$  statistical attributes per region, and  $N_{Feat}=3$  signal attributes per region (4.2). The composite fingerprint feature vector  $f_{TD}[n]$  serves as the input sequence to the anomaly detection process.

$$N_D = (N_R + 1) \times N_{Stat} \times N_{Feat} \quad (4.2)$$

*4.4.1 Single Device,  $N_B=60$ ,  $N_{Op}=5$ .* The anomaly detection process in Section 4.3.2 was repeated using the same  $N_B=60$  bursts per operating condition for the *Norm*, *Anom #1*, and *Anom #2*  $N_{Op}=5$  conditions. There were  $N_{Tng}=3$  bursts per operating condition selected for training and  $N_{Tst}=57$  bursts per operating condition selected for testing to evaluate CBAD processing. The multiple burst processing was repeated for  $SNR \in [-25.0, 25.0]$  dB using  $N_{Nr}=10$  AWGN noise realizations per  $SNR$ . This yielded a total of  $N_z=570$  test statistics for each set of RF-DNA feature vectors  $\{f_{TD1}[n], f_{TD2}[n], \dots, f_{TD570}[n]\}$  under each operating condition at each  $SNR$  considered. The process varies from the TD Waveform process in that a Composite Fingerprint  $f_{TD}$  is generated for each of the waveforms. The Composite Fingerprint is used as the input sequence to the anomaly detector.

Figure 4.6 shows the resultant  $SNR$  vs.  $TADR$  for  $SNR \in [-25.0, 25.0]$  dB. As indicated, the  $TADR_B \geq 90.0\%$  benchmark is achieved for  $SNR \geq 8.2$  dB.

Based on performance in Fig. 4.6, ROC curve performance for the  $N_B=60$  case was assessed for  $SNR=8.2$  dB. The resultant ROC curve in Fig. 4.7 shows  $EER \leq 10.0\%$  which satisfies the  $EER_B \leq 10.0\%$  benchmark.

TD waveform magnitude sequences  $|x[n]|$  are not an effective input for the CBAD process due to variation between collected bursts. When evaluating the po-

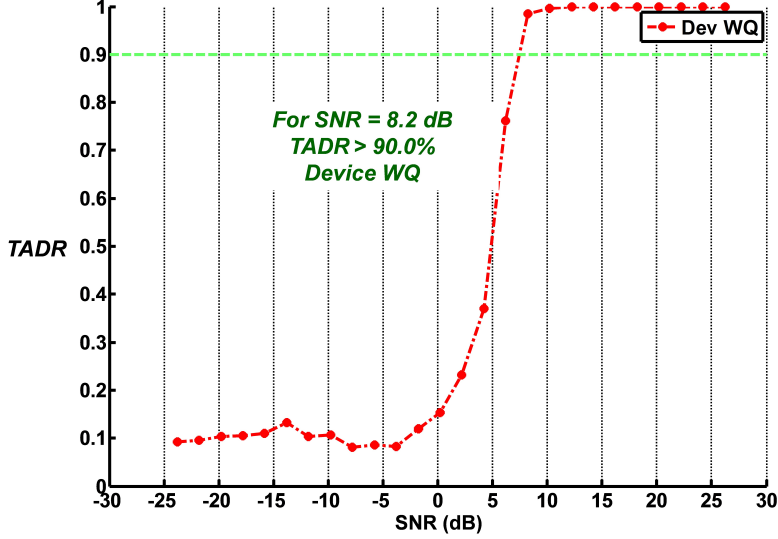


Figure 4.6:  $SNR$  vs.  $TADR$  performance using TD magnitude sequence  $|x[n]|$  for  $N_B=60$  bursts with the PLC operating under  $Norm$ ,  $Anom$  #1, and  $Anom$  #1 conditions using  $N_{OP}=5$  LLP operations. The  $TADR_B > 90.0\%$  benchmark is achieved for  $SNR \geq 8.2$  dB.

tential for using the RF-DNA features as input sequences, a specific feature sequence  $f_{RTD}$  was selected as the reference based on observed  $TADR$  performance. The results indicate that using the RF-DNA features  $f_{TD}[n]$  as input sequences results in improved performance when compared to using the TD waveform magnitude sequences as inputs when the reference burst is specifically selected based on analysis of the normal *and* anomalous bursts. The envisioned approach is for the training to rely on the *known* normal bursts only.

Figure 4.8 shows  $TADR$  results for  $SNR \in [-30.0, 30.0]$  dB using the CBAD reference selection process to automatically select the reference training burst training on observed normal conditions only. The  $TADR_B \geq 90.0\%$  benchmark is not achieved for any  $SNR \in [-30.0, 30.0]$  dB.

The resultant  $TADR$  performance in Fig. 4.8 is poorer than the  $TADR_B \geq 90.0\%$  benchmark for all  $SNR$  considered. Given that  $SNR=30.0$  dB yielded the highest  $TADR$ , it was used to generate the ROC curve results for the  $N_B=60$  case shown in

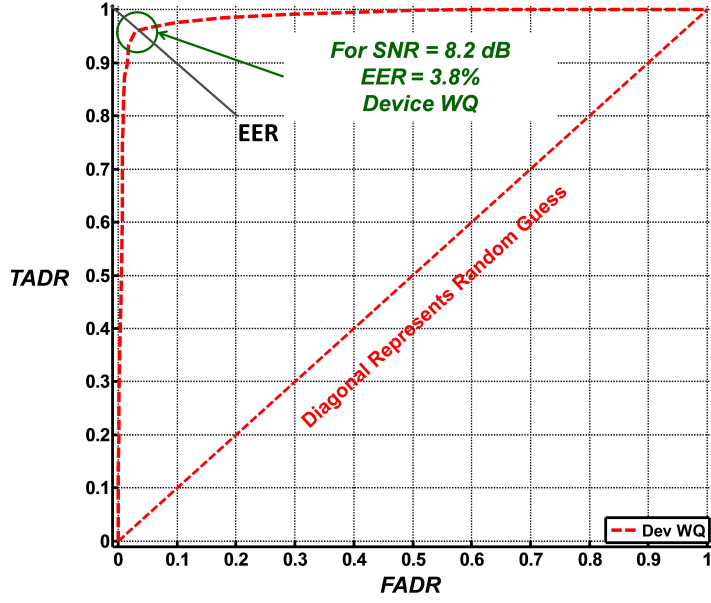


Figure 4.7: Anomaly detection ROC curve for  $SNR=8.2$  dB operating point in Fig. 4.6. Results obtained using TD RF-DNA feature sequences  $f_{TD}[n]$  for  $N_B=60$  bursts with the PLC operating under *Norm*, *Anom* #1, and *Anom* #1 conditions using  $N_{OP}=5$  LLP operations. The  $EER_B \leq 10.0\%$  benchmark is achieved.

Fig. 4.9. The  $EER_B \leq 10.0\%$  benchmark is not achieved for any  $SNR \in [-30.0, 30.0]$  dB.

Using the feature-based detection, the selection of the reference burst substantially affects performance. In the envisioned use-case, the reference would be built based on observed *normal* operation using an automated process. A more robust method of detecting anomalous behavior is required.

**Performance:** The *RF-DNA Feature Sequences* were insufficient for reliably detecting anomalous operating conditions and the desired benchmark performance was not achieved using multiple bursts [87, 89].

#### 4.5 Software Anomaly Detection: Hilbert Sequences

The failure of the anomaly detection process for multiple collected response waveforms using waveforms and the lack of robust characteristics when using features necessitates another means of representing the anomalous and normal operating

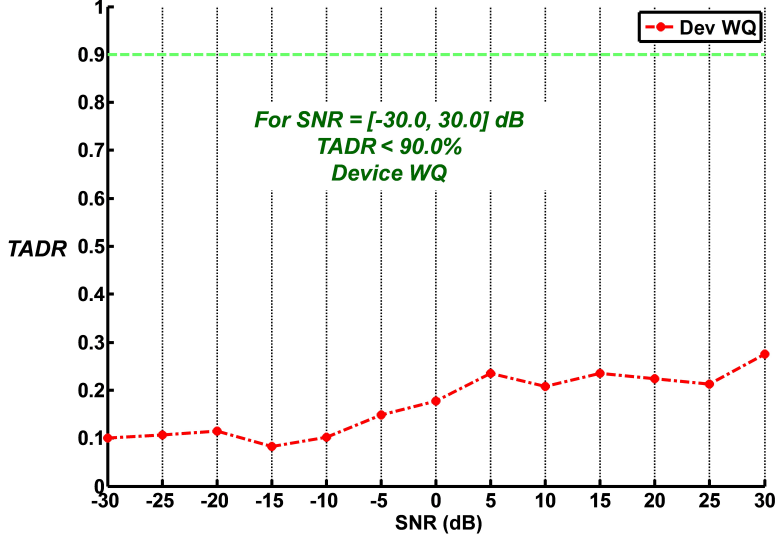


Figure 4.8:  $SNR$  vs.  $TADR$  performance using TD magnitude sequence  $|x[n]|$  for  $N_B=60$  bursts with the PLC operating under  $Norm$ ,  $Anom$  #1, and  $Anom$  #1 conditions,  $N_{OP}=5$  LLP operations, with training only based on  $Norm$  input sequences. The  $TADR_B > 90.0\%$  benchmark is not achieved for any  $SNR \in [-30.0, 30.0]$  dB.

conditions. Recall the Hilbert transform used in audio signal processing applications to stabilize signal's amplitude estimates [31, 71]. The next step in this research effort is to evaluate the feasibility of using the Hilbert transform to improve anomaly detection performance. The Hilbert transform is performed as specified in Section 3.6.1 on TD waveform sequences,  $x[n]$  to generate Hilbert transformed magnitude sequences,  $|H[x[n]]|$ . The input sequence for TD-Based anomaly detection is the magnitude of the collected real-valued TD emission,  $|x[n]|$ . For brevity, the sequences are denoted as *TD sequences*  $|x[n]|$  to differentiate from corresponding *Hilbert sequences*  $|H[x[n]]|$ .

**4.5.1 Single Device,  $N_B=60$ ,  $N_{Op}=5$ .** To evaluate the impact of using noise degraded signals in the anomaly detection process, the CBAD process is performed using Hilbert transformed magnitude input sequences  $|H[x[n]]|$  generated by taking the Hilbert transform of TD waveform sequences combined with AWGN sequences

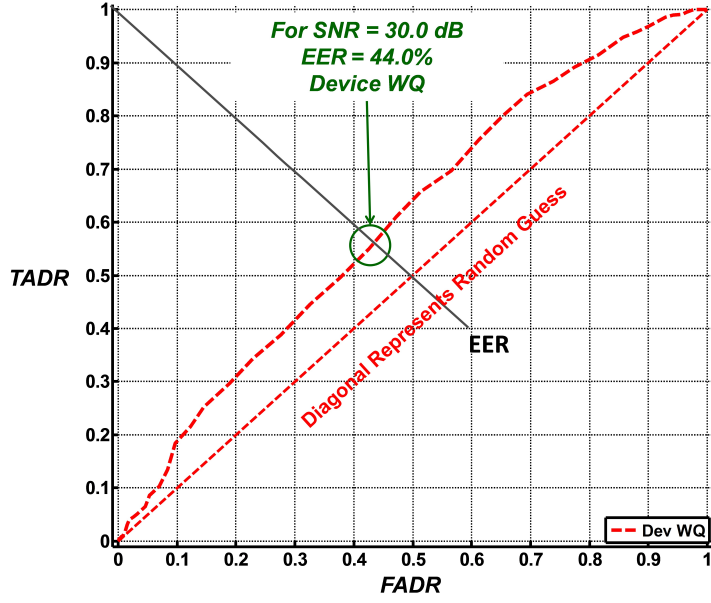


Figure 4.9: Anomaly detection ROC curve for  $SNR=30.0$  dB operating point in Fig. 4.8. Results obtained using TD RF-DNA feature sequences  $f_{TD}[n]$  for  $N_B=60$  bursts with the PLC operating under *Norm*, *Anom #1*, and *Anom #1* conditions using  $N_{OP}=5$  LLP operations. The  $EER_B \leq 10.0\%$  benchmark is not achieved.

to for  $SNR \in [-30.0, 30.0]$  dB as in the waveform input sequence analysis. There are a total  $N_B=60$  TD waveforms with  $N_{Tng}=3$  bursts selected as training burst, leaving  $N_{Tst}=57$  bursts per operating condition for CBAD processing evaluation. For each  $SNR$  considered, the anomaly detection process used  $N_{Nr}=10$  AWGN realizations per  $SNR$ . This yielded a total of  $N_z=570$  Hilbert sequences and associated CBAD test statistics for each permutation of operating condition, device, and  $SNR$  considered.

Figure 4.3 shows results for the anomaly detection process when the TD sequences are used as inputs. Using the TD sequences results in an unacceptable anomaly detection rate of  $TADR \leq 90.0\%$  for all  $SNR$  considered.

The anomaly detection process was repeated using the same  $N_B=60$  collected PLC emissions per operating condition, per device, under the *Norm*, *Anom #1*, and *Anom #1* operating conditions. The same  $SNR$  and same AWGN noise realizations



were used for each operating condition and each device to generate the Hilbert magnitude sequences  $\{|H[x_1[n]]|, |H[x_2[n]]|, \dots |H[x_{60}[n]]|\}$ .

Figure 4.10 shows results for the TADR at  $SNR \in [-30.0, 30.0]$  dB when the Hilbert sequences  $|H[x[n]]|$  are used as inputs. The  $TADR_B \geq 90.0\%$  benchmark is achieved for  $SNR \geq 0.0$  dB.

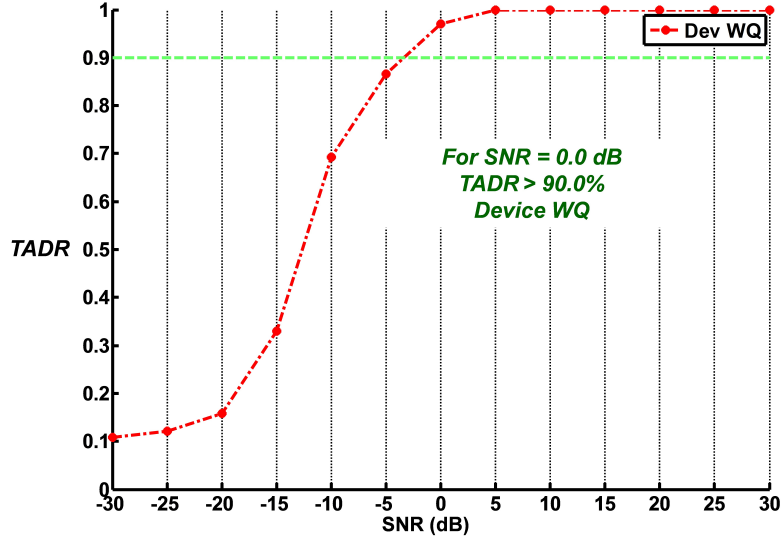


Figure 4.10:  $SNR$  vs.  $TADR$  performance using Hilbert magnitude sequences  $|H[x[n]]|$  for  $N_B=60$  bursts with the PLC operating under *Norm*, *Anom #1* and *Anom #1* conditions using  $N_{OP}=5$  LLP operations, with training only based on *Norm* input sequences. The  $TADR_B > 90.0\%$  benchmark is achieved for  $SNR \geq 0.0$  dB.

Based on performance in Fig. 4.10, ROC curve performance for the  $N_B=60$  case was assessed for  $SNR=0.0$  dB. The resultant ROC curve in Fig. 4.11 shows that the  $EER_B \leq 10.0\%$  benchmark was achieved.

**4.5.2 Ten Devices,  $N_B=1000$ ,  $N_{Op}=10$ .** Previous results were based on input sequences  $x[n]$  from a single PLC device (*WQ*) using the  $N_{OP}=5$  LLP operations shown in Fig. 2(a). For the following results, the device pool was increased to  $N_{Dev}=10$  PLC devices  $\{WQ, WV, KG, QI, KV, OV, RG, ZC, ZZ, ZA\}$  of the same

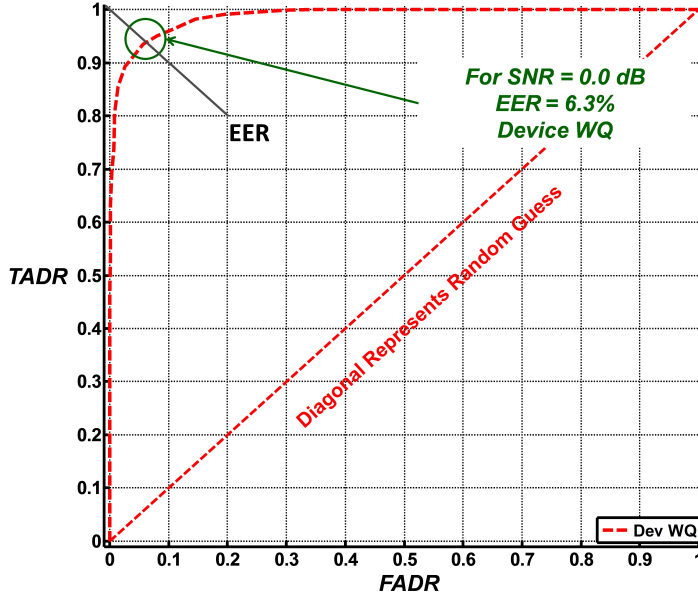


Figure 4.11: Anomaly detection ROC curve for  $SNR=0.0$  dB operating point in Fig. 4.10. Results obtained using Hilbert magnitude sequences  $|H[x[n]]|$  for  $N_B=60$  bursts with the PLC operating under *Norm*, *Anom #1*, and *Anom #1* conditions using  $N_{OP}=5$  LLP operations. The  $EER_B \leq 10.0\%$  benchmark is achieved.

brand and model number as summarized in Table 3.1. Additionally, the LLPs used for simulating *Norm*, *Anom #1*, and *Anom #2* operating conditions was based on the  $N_{OP}=10$  operations shown in Fig. 2(b).

To evaluate the impact of using noise degraded signals with the anomaly detection process, CBAD processing was performed using Hilbert transformed input sequences  $|H[x[n]]|$  generated by taking the Hilbert transform of TD waveform sequences combined with AWGN sequences for  $SNR \in [-30.0, 30.0]$  dB as in the waveform input sequence and previous Hilbert Transform-based emissions. Results in previous sections were based on either  $N_B=1$  or  $N_B=60$  bursts. The anomaly detection process was performed using  $N_B=1000$  collected PLC emissions per operating condition per device for the *Norm*, *Anom #1*, and *Anom #2* operating conditions. A total of  $N_{Tng\%}=5\%$  or  $N_{Tng}=50$  Hilbert sequences were selected as training bursts, leaving  $N_{Tst}=950$  sequences per operating condition for the CBAD processing evaluation. For each  $SNR$  considered, the anomaly detection process was implemented

using  $N_{Nr}=10$  AWGN noise realizations per  $SNR$ . This yielded  $N_z=9500$  total test statistics for each permutation of operating condition, device, and  $SNR$  considered. The same  $SNR$  levels and AWGN noise realizations for each operating condition for each device at each  $SNR$  were used to generate the Hilbert test sequences  $\{|H[x_1[n]]|, |H[x_2[n]]|, \dots |H[x_{950}[n]]|\}$ .

Figure 4.12 shows results for the TADR at  $SNR \in [-30.0, 30.0]$  dB when the Hilbert sequences  $|H[x[n]]|$  are used as inputs. The  $TADR_B \geq 90.0\%$  benchmark is achieved for  $SNR \geq 5.0$  dB and all  $N_{Dev}=10$  devices.

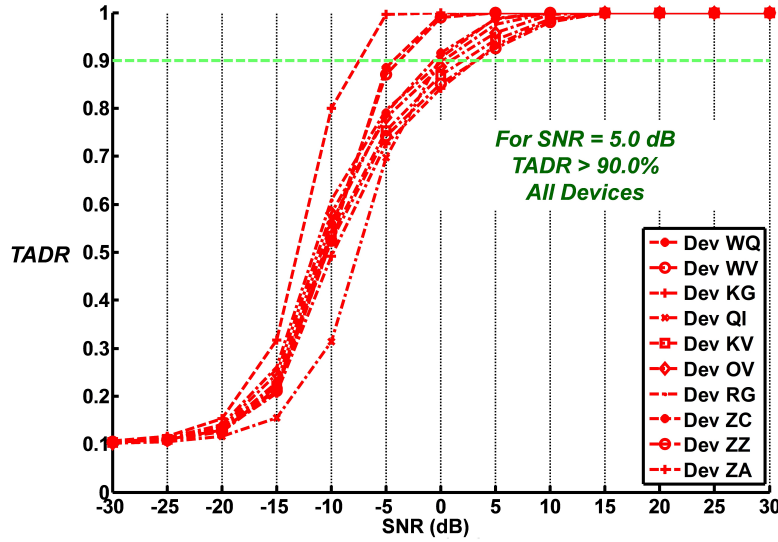


Figure 4.12:  $SNR$  vs.  $TADR$  performance using Hilbert magnitude sequences  $|H[x[n]]|$  for  $N_B=1000$  bursts with all PLCs operating under *Norm*, *Anom* #1 and *Anom* #1 conditions using  $N_{OP}=10$  LLP operations, with training only based on *Norm* input sequences. The  $TADR_B \geq 90.0\%$  benchmark is achieved for all devices at  $SNR \geq 5.0$  dB.

Based on performance in Fig. 4.12, ROC curve performance for the  $N_B=1000$  case was assessed for  $SNR=5.0$  dB. The resultant ROC curve in Fig. 4.13 shows that the arbitrary  $EER_B \leq 10.0\%$  benchmark is achieved for all  $N_{Dev}=10$  considered.

Anomaly detection ROC curves for  $SNR=5.0$  dB operating point in Fig. 4.13 demonstrate results obtained using Hilbert magnitude sequences  $|H[x[n]]|$  for  $N_B=1000$

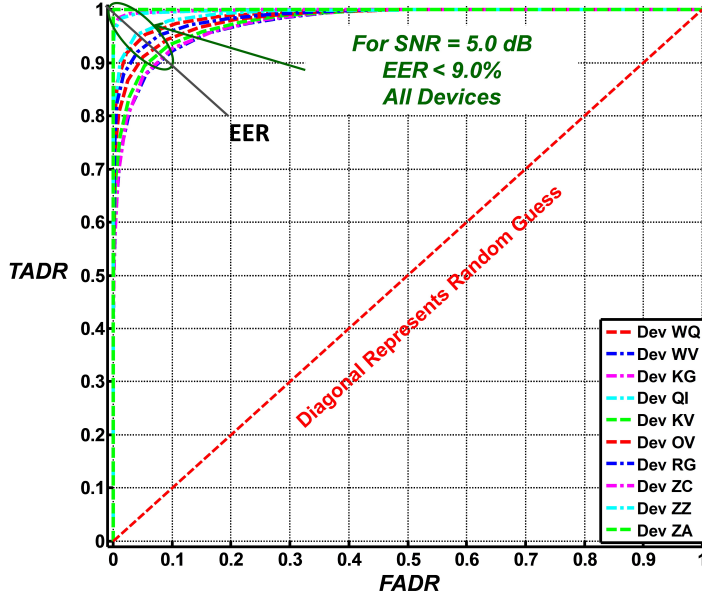


Figure 4.13: Anomaly detection ROC curves for  $SNR=5.0$  dB operating point in Fig. 4.12. Results obtained using Hilbert magnitude sequences  $|H[x[n]]|$  for  $N_B=1000$  bursts with the PLCs operating under *Norm*, *Anom #1*, and *Anom #1* conditions using  $N_{OP}=10$  LLP operations. The  $EER_B \leq 10.0\%$  benchmark is achieved for all devices.

bursts with the PLCs operating under *Norm*, *Anom #1*, and *Anom #1* conditions using  $N_{OP}=10$  LLP operations. The  $EER_B \leq 10.0\%$  benchmark is achieved for all devices.

**Performance:** The *Hilbert Transform Feature Sequences* with *cross-operation* CBAD processing were sufficiently robust for reliably detecting anomalous operating conditions. The desired  $TADR_B \geq 90.0\%$  and  $EER_B \leq 10.0\%$  performance benchmarks were achieved using 1)  $N_B=60$  sequences for  $SNR \geq 0.0$  dB, and 2)  $N_B=1000$  sequences for  $SNR \geq 5.0$  dB.

The operation-by-operation CBAD processing in Sect. 3.9 effectively weights the differences for each operation (as quantified by CBAD statistic  $z_V$ ) equally irrespective of how much of the total operating condition sequence is attributable to the specific operation.

Figure 4.14 shows results for the TADR at  $SNR \in [-30.0, 30.0]$  dB when the Hilbert sequences  $|H[x[n]]|$  are used as inputs and CBAD statistics are calculated for each operation region  $\{Reg_{OP1}, Reg_{OP2}, \dots, Reg_{OP10}\}$ . The  $TADR_B \geq 90.0\%$  benchmark is achieved for  $SNR \geq 0.0$  dB for all  $N_{Dev}=10$  considered. This represents a gain of  $SNR_{Gain}=5.0$  dB when compared with the results without using the operation-by-operation process.

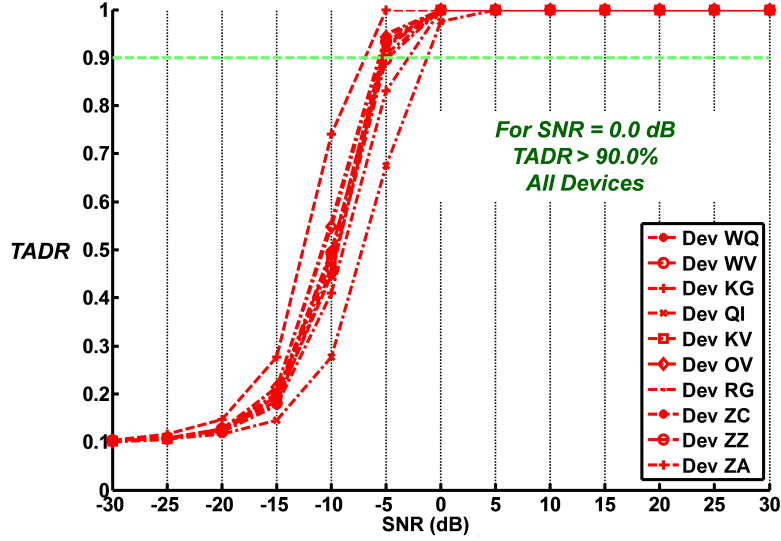


Figure 4.14:  $SNR$  vs.  $TADR$  performance for *Operation-by-Operation CBAD Processing* using Hilbert magnitude sequences  $|H[x[n]]|$ . Results for  $N_B=1000$  bursts with all PLCs operating under *Norm*, *Anom* #1 and *Anom* #1 conditions using  $N_{OP}=10$  LLP operations. The  $TADR_B > 90.0\%$  benchmark is achieved for all devices at  $SNR \geq 0.0$  dB.

Based on performance in Fig. 4.14, ROC curve performance for the  $N_B=1000$  case was assessed for  $SNR=0.0$  dB. The resultant ROC curve in Fig. 4.15 shows an  $EER \leq 6.3\%$  for all  $N_{Dev}=10$  devices and the  $EER_B \leq 10.0\%$  benchmark is achieved.

Anomaly detection ROC curves for *Operation-by-Operation CBAD Processing* at  $SNR=0.0$  dB operating point are shown in Fig. 4.15. Results are obtained using Hilbert magnitude sequences  $|H[x[n]]|$  for  $N_B=1000$  bursts with the PLCs operating

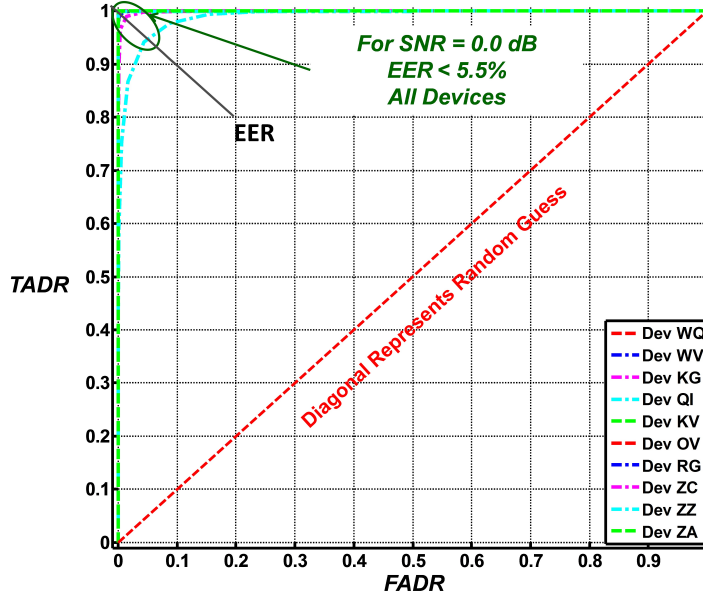


Figure 4.15: Anomaly detection ROC curves for *Operation-by-Operation CBAD Processing* at  $SNR=0.0$  dB operating point in Fig. 4.14. Results obtained using Hilbert magnitude sequences  $|H[x[n]]|$  for  $N_B=1000$  bursts with the PLCs operating under *Norm*, *Anom #1*, and *Anom #1* conditions using  $N_{OP}=10$  LLP operations. The  $EER_B \leq 10.0\%$  benchmark is achieved for all devices.

under *Norm*, *Anom #1*, and *Anom #1* conditions using  $N_{OP}=10$  LLP operations. The  $EER_B \leq 10.0\%$  benchmark is achieved for all devices.

**Performance:** The *Hilbert Transform Feature Sequences* with *operation-by-operation* CBAD processing were sufficiently robust for reliably detecting anomalous operating conditions. The  $TADR_B \geq 90.0\%$  and  $EER_B \leq 10.0\%$  benchmarks were achieved using  $N_B=1000$  sequences for  $SNR \geq 0.0$  dB; a 5.0 dB gain relative to performance using *cross-operation* CBAD processing.

#### 4.6 Hardware Component Discrimination

Results in the preceding sections focused on *software anomaly detection* in PLC devices—discriminating between various *operating conditions* to detect malfunctioning or malicious software, firmware, etc. A complementary application emerged as the research progressed and the verification-based anomaly detection process was ap-

plied to support *hardware component discrimination*—discriminating between various *hardware components* to detect malfunctioning or counterfeit, trojan, etc., Integrated Circuits (IC) such as commonly used in PLCs.

Hardware component discrimination was assessed using the GRLVQI process as developed and verified in [76]; the process was implemented here as published without any modification. From a fundamental classification perspective, the GRLVQI model development and verification process is “signal agnostic” and can accept any collection of input sequences. Thus, for consistency and comparison with previous *software anomaly detection* results, two different input sequence types were considered for *hardware component discrimination*: 1) Time Domain (TD) feature sequences and 2) Correlation Domain (CD) feature sequences.

The TD RF-DNA sequences  $f_{TD}[n]$  were generated in the same manner described in Sect. 4.4 and contained  $N_D=156$  features. The statistical features were generated using the RF-DNA process in Sect. 3.6.2 with TD  $x[n]$  sequences as inputs. GRLVQI performance was also assessed using CD feature sequences  $f_{CD}[n]$  that were generated using the Operation-by-Operation CBAD process in Sect. 3.9. Instead of creating a single CBAD statistic  $z_V$ , a vector of CBAD statistics  $\{z_{1V}, z_{2V}, \dots, z_{N_{10V}}\}$  was generated from the  $N_{Op}=10$  LLPs. These resultant CBAD statistical sequences  $f_{CD}[n]=\{z_{1V}, z_{2V}, \dots, z_{N_{10V}}\}$  were used as inputs for GRLVQI verification performance assessment.

*4.6.1 GRLVQI Verification: TD Sequences.* The initial hardware discrimination is performed using RF-DNA features extracted from the TD waveform sequences  $\{x_1[n], x_2[n], \dots, x_{N_B}[n]\}$ ,  $N_B=1000$ . There are a total of  $N_{Tng}=500$  TD waveform sequences used, leaving  $N_{Tst}=500$  TD waveforms for testing. The training and testing waveforms are combined with  $N_{Nr}=10$  AWGN realizations per  $x[n]$  sequence.

Devices were divided into two arbitrary classes, including the 1) *authorized* hardware devices ( $\{WQ, WV, KV, OV, RG\}$ ) and the unauthorized 2) *rogue* hardware devices ( $\{KG, QI, ZA, ZC, ZZ\}$ ). For this research, *authorized devices* refers to the set of hardware devices  $\{WQ, WV, KV, OV, RG\}$  which are considered *normal* or *non-anomalous* while *rogue devices* refers to the set of hardware devices  $\{KG, QI, ZA, ZC, ZZ\}$  which are considered *anomalous*. In reality, all devices are assumed to be non-counterfeit and are purchased through normal commercial channels. For both *Authorized Device Verification* and *Rogue Device Rejection* assessment the GRLVQI verification model was developed using only authorized device training sequences. In addition, when performing *Rogue Device Rejection* assessment achieving the  $EER_B \leq 10.0\%$  benchmark is equivalent to achieving a Rogue Rejection Rate (RRR) of  $RRR > 90.0\%$ .

RF-DNA features were extracted using the processes of *Feature Extraction* and *Statistical Fingerprint Generation* are used to create a *Composite Fingerprint* based on the waveform [11, 76, 103] and outlined in Section 3.6.2. The Composite Fingerprint reduces the dimensionality of the sequence used in the anomaly detection process. The waveform sequences considered for this research are represented by an  $N_D=15880$  dimensional vector. The dimensionality of the waveform-based sequence vector is based on the sampling rate  $f_s$  and time length  $T_{WF}$  of the TD waveform using 4.1.

The process graphically demonstrated in Fig. 3.11 results in a  $N_D=156$  dimensional vector using  $N_R=12$  sub regions and the total signal,  $N_{Stat}=4$  statistical attributes per region, and  $N_{Feat}=3$  signal attributes per region (4.2). The composite fingerprint feature vector serves as the input sequence to the anomaly detection process.

The *Authorized Device Verification* capability of GRLVQI processing was first evaluated using TD RF-DNA sequences  $f_{TD}[n]$  with the  $\{WQ, WV, KV, OV, RG\}$  PLCs serving as authorized devices, i.e., devices from which emission sequences are



extracted and used for model development. Recall that in the general verification process in Chapter 3 dictates that each device or operation has a *claimed* identity and *actual* identity. Figure 4.16 shows *Authorized Device Verification* ROC curve results for  $SNR=15.0$  dB using TD feature sequences  $f_{TD}[n]$  as input to the GRLVQI process. The claimed and actual identities are equal. The ROC curve results are a measure of how similar an authorized device resembles the other authorized devices in the test as compared to how closely the device resembles itself. A low *EER* equates to a device with a unique set of features that are not commonly mistaken for features from another device. A high *EER* equates to a device that with a set of features that are similar to the other devices in the test.

For the case of authorized device discrimination, the  $EER_B \leq 10.0\%$  benchmark is achieved for all of the devices at  $SNR=15.0$  dB.

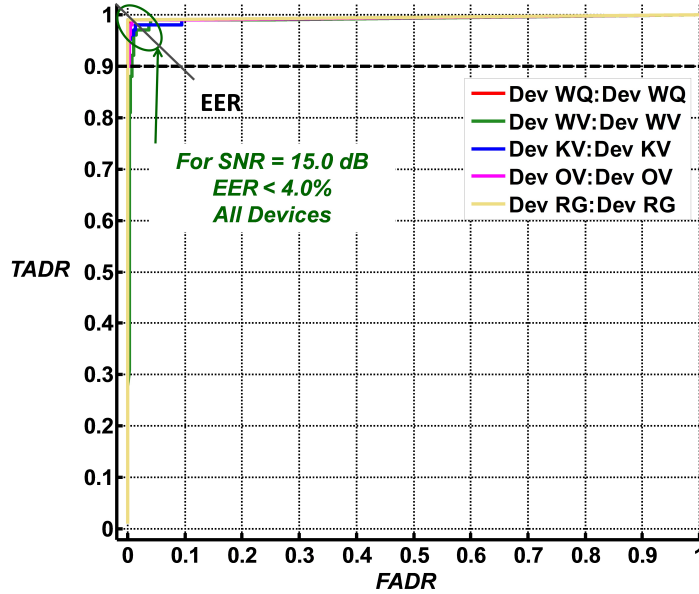


Figure 4.16: GRLVQI hardware component discrimination ROC curves for *Authorized Device Verification* using the  $\{WQ, WV, KV, OV, RG\}$  PLCs with TD RF-DNA sequences  $f_{TD}[n]$ . Results for  $SNR=15.0$  dB using  $N_B=1000$  bursts with the PLCs operating under *Norm*, *Anom #1*, and *Anom #1* conditions using  $N_{OP}=10$  LLP operations. The  $EER_B \leq 10.0\%$  benchmark is achieved with  $EER \leq 4\%$  for all devices.

The GRLVQI process was next evaluated to assess *Rogue Device Rejection* capability using TD RF-DNA sequences  $f_{TD}[n]$  with the  $\{WQ, WV, KV, OV, RG\}$  PLCs serving as rogues, i.e., devices which have not been previously seen nor used for authorized device model development. Figure 4.17 shows *Rogue Devices* ROC curve results for  $SNR=15.0$  dB using TD features as in the GRLVQI process. The claimed and actual device IDs are not the same and the ROC curve results are presented as represent DevX:DevY (*Actual:Claimed*) ID pairs. The GRLVQI process was evaluated with each one of the rogue devices presenting a claimed ID for all five authorized devices. Thus, there were a total of 25 DevX:DevY ID pairs considered. For visual clarity, the legend is not displayed in Fig. 4.17. The ROC curve results are a measure of how much a rogue device resembles an authorized devices in the test. A low *EER* indicates a rogue device is unlikely to be falsely verified as an authorized device. A high *EER* indicates a rogue device is likely to be accepted/authorized as an authorized device.

For the case of *Rogue Device Rejection*, the  $EER_B \leq 10.0\%$  benchmark was achieved at  $SNR=15.0$  dB for all of device pairs. For all devices except the *KG:WQ* pair, the  $EER \leq 3.0\%$ . For the *KG:WQ* pair, the  $EER \approx 9.0\%$ . This is a result of RF-DNA features from device *KG* being most similar to the *WQ* RF-DNA features and there is a higher likelihood that rogue *KG* would be being falsely verified as authorized device *WQ* than any other rogue device being falsely verified as another authorized device.

**4.6.2 GRLVQI Verification: CD Sequences.** The second and final hardware discrimination evaluation is performed using CBAD statistics extracted from the Hilbert Transform sequences  $\{|H[x_1[n]]|, |H[x_2[n]]|, \dots, |H[x_{N_B}[n]]|\}$ ,  $N_B=1000$  combined with  $N_{Nr}=10$  AWGN realizations per  $x[n]$  sequence, *authorized* hardware devices ( $\{WQ, WV, KV, OV, RG\}$ ) and *rogue* hardware devices ( $\{KG, QI, ZA, ZC, ZZ\}$ ). For this research effort, the term *authorized devices* refers to the set of hardware devices  $\{WQ, WV, KV, OV, RG\}$ , which are considered *normal* or *non-*

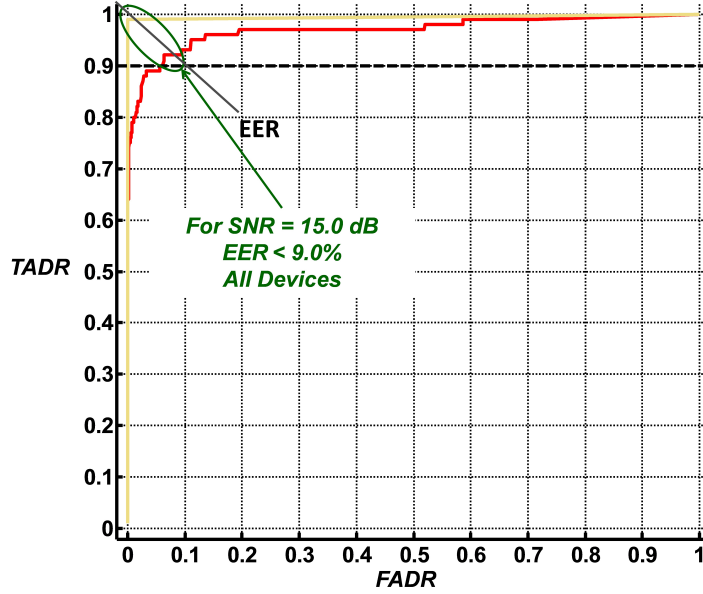


Figure 4.17: GRLVQI hardware component discrimination ROC curves for *Rogue Device Rejection* using TD RF-DNA sequences  $f_{TD}[n]$ . The DevX:DevY legend notation has been omitted for visual clarity. Results are for  $SNR=15.0$  dB using  $N_B=1000$  bursts with the PLCs operating under *Norm*, *Anom #1*, and *Anom #1* conditions using  $N_{OP}=10$  LLP operations. The  $EER_B \leq 10.0\%$  benchmark is achieved for all cases. The highest  $EER_{KG:WQ} \approx 9.0\%$  is for the pair  $KG:WQ$  –a consequence of  $KG$  and  $WQ$  RF-DNA features being most similar.

*anomalous*. The term *rogue devices* refers to the set of hardware devices  $\{KG, QI, ZA, ZC, ZZ\}$ , which are considered *anomalous*.

Previously, statistical RF-DNA features were successfully used as the input sequences for GRLVQI processing. For this research, the input sequences are generated using the CBAD process to generate a set of CBAD CD statistics  $\{z_{1V}, z_{2V}, \dots, z_{N_{OP}V}\}$ ,  $N_{OP}=10$  with each CBAD statistic generated from the signal content for one of the operations in the LLP. Each CBAD statistic was generated using the process described in Section 4.5.2. As is the case for the RF-DNA feature extraction, the CBAD statistic process reduces the dimensionality of the sequence used in the anomaly detection process. The waveform sequences considered for this research are represented by an  $N_D=15880$  dimensional vector. The dimensionality of the waveform-based sequence vector is based on the sampling rate  $f_s$  and time length

$T_{WF}$  of the TD waveform 4.1. The CBAD statistic vectors are  $N_D=10$  dimensional vectors. When compared to the TD RF-DNA features, the CBAD CD RF-DNA features are less than  $1/15^{th}$  the size for identical input  $x[n]$  sequences.

The *Authorized Device Verification* capability of GRLVQI processing was next evaluated using CD RF-DNA sequences  $f_{CD}[n]$  with the  $\{WQ, WV, KV, OV, RG\}$  PLCs serving as authorized devices, i.e., devices from which emission sequences are extracted and used for model development. Figure 4.18 shows the *authorized devices* ROC curve for  $SNR=15.0$  dB with TD features input to the GRLVQI process. The claimed and actual identities are equal.

For the case of authorized device verification, the  $EER_B \leq 10.0\%$  benchmark is achieved for all of the devices except for devices  $\{KV, WV\}$  at  $SNR=15.0$  dB. CBAD statistic vectors for *authorized* devices  $KV$  and  $WV$  are similar to other *authorized* devices in the test.

The final GRLVQI assessment included *Rogue Device Rejection* capability using CD RF-DNA sequences  $f_{CD}[n]$  with the  $\{KG, QI, ZA, ZC, ZZ\}$  PLCs serving as rogue devices, i.e., devices which have not been previously seen nor used for authorized device model development. Figure 4.19 shows *rogue device* ROC curve results for  $SNR=15.0$  dB using CBAD statistic vectors as input to the GRLVQI process. As in the RF-DNA features case, there are a total of  $N_{Perm}=25$  permutations when considering *Actual:Claimed* identity pairs for authorized device set  $\{WQ, WV, KV, OV, RG\}$  and rogue device set  $\{KG, QI, ZA, ZC, ZZ\}$ .

For the case of rogue device detection, the  $EER_B \leq 10.0\%$  benchmark is achieved for all of the devices pairs at  $SNR=15.0$  dB. As is the case for RF-DNA features, the CBAD statistic vectors for device  $KG$  are most similar to the CBAD statistic vectors for the *authorized* devices. Device  $KG$  most closely resembling  $WQ$  equating to a higher likelihood of the rogue device  $KG$  being falsely verified as the authorized device  $WQ$  than the other authorized device.

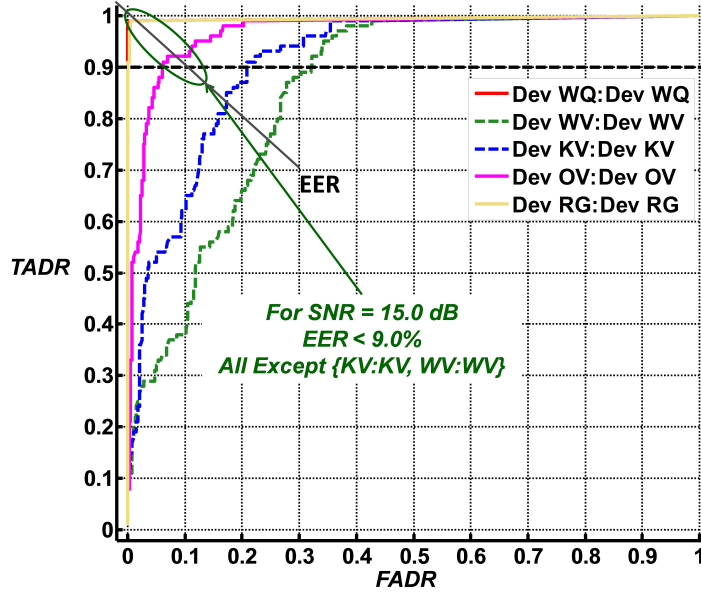


Figure 4.18: GRLVQI hardware component discrimination ROC curves for *Authorized Device Rejection* using the  $\{WQ, WV, KV, OV, RG\}$  PLCs with CD feature sequences  $f_{CD}[n]$ . Results for  $SNR=15.0$  dB using  $N_B=1000$  bursts with the PLCs operating under *Norm*, *Anom #1*, and *Anom #1* conditions using  $N_{OP}=10$  LLP operations. The  $EER_B \leq 10.0\%$  benchmark is achieved for all devices except  $\{KV, WV\}$ —a consequence of  $KV$  and  $WV$  CD features being relatively similar to other authorized devices.

**Performance:** With the exception of assessments involving the CBAD features for  $\{KV, WV\}$  devices and authorized device discrimination, GRLVQI processing using both TD RF-DNA and CD CBAD input sequences was effective for verifying authorized device IDs with the  $EER_B \leq 10.0\%$  benchmark achieved for  $SNR=15.0$  dB. The  $\{KV, WV\}$  device CBAD features were insufficiently distinct from each of the authorized devices. Both TD RF-DNA and CD CBAD input sequences were effective for performing *Actual:Claimed* rogue ID assessment, with the  $EER_B \leq 10.0\%$  benchmark achieved for  $SNR=15.0$  dB.

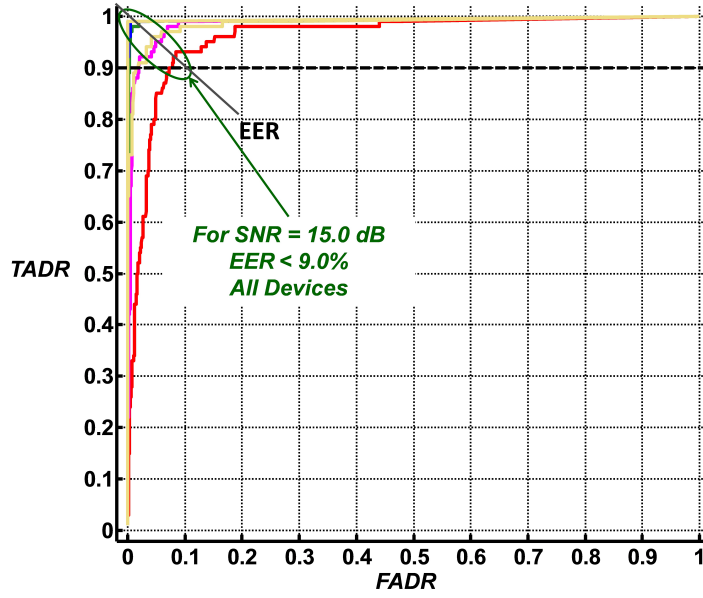


Figure 4.19: GRLVQI hardware component discrimination ROC curves for *Rogue Device Rejection* using CD RF-DNA sequences  $f_{TD}[n]$ . The DevX:DevY legend notation has been omitted for visual clarity. Results are for  $SNR=15.0$  dB using  $N_B=1000$  bursts with the PLCs operating under *Norm*, *Anom #1*, and *Anom #1* conditions using  $N_{OP}=10$  LLP operations. The highest  $EER_{KG:WQ} \approx 9.0\%$  is for the pair *KG:WQ* –a consequence of *KG* and *WQ* CD features being most similar.

## 5. Conclusion

This chapter provides a summary of research activity and results for development and demonstration of a verification-based anomaly detection approach that supports 1) *software anomaly detection*—discriminating between various *operating conditions* to detect malfunctioning or malicious software, firmware, etc., and 2) *hardware component discrimination*—discriminating between various *hardware components* to detect malfunctioning or counterfeit, trojan, etc., Integrated Circuits (IC).

Section 5.1 provides a research summary in support of providing results and conclusions for 1) the proposed Correlation Based Anomaly Detection (CBAD) process in Sect. 5.2 which was used to assess device *operating condition discrimination* and 2) the Generalized Relevance Learning Vector Quantized-Improved (GRLVQI) process in Sect. 5.3 which was used to assess *hardware component discrimination*. The chapter concludes with recommendations for future research in Sect. 5.4 which are motivated by the research developments and demonstrations completed herein.

### 5.1 Research Summary

Supervisory Control And Data Acquisition (SCADA) systems remain vulnerable to malicious cyber attacks [13, 33, 44, 60, 93, 94] and are an integral element of critical infrastructures in the United States and around the world. They are responsible for controlling activities from waste-water treatment to nuclear power generation. The concern over these vulnerabilities is greatest when considering the critical nature of SCADA when integrated within an Industrial Control System (ICS). The current and previous US presidents have highlighted the critical nature of SCADA security through presidential directives and executive orders directing efforts toward securing critical infrastructure facilities and systems [5, 66]; despite this motivation and related technical advancements legacy SCADA systems remain vulnerable.

One key vulnerability rests within Programmable Logic Controller (PLC) devices that are used to implement low-level SCADA and ICS functions such as operating valves, monitoring temperatures, activating relays, etc. PLCs provided the avenue through which recent SCADA cyber attacks have been orchestrated [12, 105] and are particularly vulnerable for two primary reasons: 1) PLCs run proprietary Operating Systems (OS) software using limited/minimal hardware; this precludes the use of Anti Virus (AV) or Intrusion Detection System (IDS) Programs, and 2) PLC devices and implementation architectures may stay in operation for decades; the lack of upgrades keep them vulnerable even as well-publicized exploits emerge.

The 7-layer Open System Interconnect (OSI) model provides a common means for describing various levels of networked infrastructure functionality [7]. While most methods securing networked systems from attack reside within the upper Network (NET) or Application (APP) model layers, this approach is problematic for many fielded systems due to the limited on-board computing resources within PLC devices. One avenue of augmenting Network/Application layer security is by exploiting information in the lower Physical (PHY) layer. This is one focus area of AFIT's Radio Frequency Intelligence (RFINT) program that has developed a solid knowledge base on targeting and exploiting PHY layer attributes to address bit-level security augmentation, device discrimination, and Side Channel Analysis (SCA) [9–11, 21, 39–42, 56–58, 74, 77, 79, 81, 91, 92, 103].

The goal of this research was to expand AFIT's RFINT technology base by developing and analyzing a process for reliably detecting anomalous activity in SCADA PLC devices using PHY layer attributes. This was addressed using a verification-based approach for both *software anomaly detection* and *hardware component discrimination* using the proposed CBAD for detecting anomalous PLC activity. The CBAD process was introduced to detect anomalous behavior that differs from observed normal behavior by *verifying* normal operations and *detecting* anomalous operations; a binary declaration process where a cause-independent determination



of abnormal is desired. The CBAD process is inherently sequence agnostic and was demonstrated for a variety of input sequence types: Time Domain (TD) [86, 87], Radio Frequency Distinct Native Attribute (RF-DNA) features [87], and Hilbert transformed TD sequences [88].

Additional research contribution was made by leveraging previous GRLVQI [76, 78] and Radio Frequency Distinct Native Attribute (RF-DNA) [9, 11, 77, 81] research to assess *hardware component discrimination* capability. In this case, the CBAD process was used to detect anomalous behavior that differs from normal behavior by *verifying* authentic hardware devices and *detecting* rogue hardware devices. The GRLVQI process was evaluated using both TD RF-DNA features and Correlation Domain (CD) features.

Performance of verification-based *software anomaly detection* and *hardware component discrimination* capability was assessed by 1) evaluating Signal-to-noise Ratio (SNR) vs. True Anomaly Detection Rate (TADR), 2) selecting a desired TADR, and 3) generating a Receiver Operating Characteristic (ROC) curve at the corresponding SNR. The resultant ROC curve Equal Error Rate (EER) point, i.e., the point at which the two errors associated with verification are equal was arbitrarily chosen for comparative assessment as common in the biometric verification [48].

**Assessment Criteria:** The arbitrary performance benchmarks for characterizing anomaly detection performance included  $TADR_B \geq 90.0\%$  and  $EER_B \leq 10.0\%$ .

## 5.2 CBAD Software Anomaly Detection

A variety of input sequences were used to evaluate the CBAD process for software anomaly detection using operating condition discrimination, each measured against two arbitrary benchmarks: 1) the lowest  $SNR$  value at which the CBAD process and given input sequence type combination yielded  $TADR \geq 90.0\%$  and 2) ROC curve  $EER \leq 10.0\%$  for the CBAD process when calculated at the  $SNR$  for which

$TADR \geq 90.0\%$  is achieved. All processing included the addition of like-filtered Additive White Gaussian Noise (AWGN) realizations that were power scaled to achieve the desired  $SNR$  in the input sequences and, in the case of a single response, simulate multiple collected emissions.

A total of six different types of sequences were input to CBAD processing to assess software anomaly detection capability. Except for the one noted exception under Type #5, all sequences were used for *cross-operation* CBAD processing assessment.

1. *Single TD Waveform Sequence*: The  $|x[n]|$  sequence was derived from a given Device Under Test (DUT) for each operating condition (*Norm*, *Anom #1*, and *Anom #1*) generated using  $N_{OP}=5$  Ladder Logic Program (LLP) operations and  $N_{Nz}=200$  AWGN realizations.
2. *Multiple TD Waveform Sequences*: A total of  $N_B=60$  TD  $|x[n]|$  were derived from a single DUT for each operating condition (*Norm*, *Anom #1*, and *Anom #1*) generated using  $N_{OP}=5$  LLPs and  $N_{Nz}=10$  AWGN realizations.
3. *Multiple RF-DNA Feature Sequences*: A total of  $N_B=60$  RF-DNA feature sequences were generated from TD waveform sequences  $x[n]$  collected from a single DUT for each operating condition (*Norm*, *Anom #1*, and *Anom #1*) generated using  $N_{OP}=5$  LLPs and  $N_{Nz}=10$  AWGN realizations.
4. *Multiple Hilbert Transforms/Single DUT*: A total of  $N_B=60$  Hilbert transformed sequences  $|H[x[n]]|$  were generated from a single DUT for each operating condition (*Norm*, *Anom #1*, and *Anom #1*) generated using the  $N_{OP}=5$  LLPs and  $N_{Nz}=10$  AWGN realizations.
5. *Multiple Hilbert Transforms/Multiple DUTs*: A total of  $N_B=1000$  Hilbert transformed sequences  $|H[x[n]]|$  were generated from  $N_{Dev}=10$  DUTs for each operating condition (*Norm*, *Anom #1*, and *Anom #1*) using  $N_{OP}=10$  LLPs and  $N_{Nz}=10$  AWGN realizations for both *cross-operation* and *operation-by-operation* CBAD processing assessment.

Results for *cross-operation* CBAD processing using Type #1 and Type #2 TD sequences were mixed, with Type #1 sequences achieving the  $TADR_B \geq 90.0\%$  and  $EER_B \leq 10.0\%$  benchmarks for all  $SNR \in [-30, 30]$ . However, performance using Type #2 TD sequences was considerably poorer with  $TADR_B \geq 90.0\%$  never achieved over the same range of  $SNR$  [87, 89].

**Performance:** The *Untransformed TD Sequences* were insufficient for reliably detecting anomalous operating conditions and the desired benchmark performance was not achieved using multiple bursts [87, 89].

Given unacceptable performance using untransformed TD sequences, Type #3 RF-DNA feature sequences were evaluated next and performance compared against the benchmarks. Results here were favorable with the  $TADR_B \geq 90.0\%$  and  $EER_B \leq 10.0\%$  benchmarks achieved for  $SNR \geq 8.2$  dB. However, these benchmarks were achieved using a specific manually selected reference sequence based on CBAD performance analysis for both *Normal Verification* and *Anomaly Detection* using each potential reference sequence. This training approach is unrealistic for the intended purpose of detecting unknown anomalies, but the results provide the most optimistic measure of achievable performance. The CBAD process was subsequently retrained using only the *Norm* sequences and the resultant CBAD processing failed to meet the  $TADR_B \geq 90.0\%$  benchmark for all  $SNR \in [-30.0, 30.0]$  dB.

**Performance:** The *RF-DNA Feature Sequences* were insufficient for reliably detecting anomalous operating conditions and the desired benchmark performance was not achieved using multiple bursts [87, 89].

The Hilbert transform-based Type #4 and Type #5 sequences were next considered given that Hilbert transforms have been successfully used in audio processing applications to stabilize signal amplitude estimates [32, 71]. Type #4 results were favorable with the  $TADR_B \geq 90.0\%$  and  $EER_B \leq 10.0\%$  benchmarks achieved for  $SNR \geq 0.0$  dB. While being likewise favorable, Type #5 results were somewhat poorer

with the  $TADR_B \geq 90.0\%$  and  $EER_B \leq 10.0\%$  benchmarks achieved for  $SNR \geq 5.0$  dB when using *cross-operation* CBAD processing.

**Performance:** The *Hilbert Transform Feature Sequences* with *cross-operation* CBAD processing were sufficiently robust for reliably detecting anomalous operating conditions. The desired  $TADR_B \geq 90.0\%$  and  $EER_B \leq 10.0\%$  performance benchmarks were achieved using 1)  $N_B=60$  sequences for  $SNR \geq 0.0$  dB, and 2)  $N_B=1000$  sequences for  $SNR \geq 5.0$  dB.

The final CBAD performance evaluation was performed using Type #5 sequences with *operation-by-operation* CBAD processing to assess anomaly detection capability. In this case, the sequences were divided into  $N_{Reg}=N_{OP}=10$  regions based on the number of samples within each operation region. Resultant Type #5 sequence assessment included successful  $TADR \geq 90.0\%$  and  $EER \leq 10.0\%$  benchmark performance at  $SNR \geq 0.0$  dB. Relative to *cross-operation* CBAD processing results introduced earlier, this represents a “gain” of 5.0 dB in performance—measured here as the reduction in required  $SNR$ , expressed in dB, for two methods based on identical inputs to achieve the same benchmark performance.

**Performance:** The *Hilbert Transform Feature Sequences* with *operation-by-operation* CBAD processing were sufficiently robust for reliably detecting anomalous operating conditions. The  $TADR_B \geq 90.0\%$  and  $EER_B \leq 10.0\%$  benchmarks were achieved using  $N_B=1000$  sequences for  $SNR \geq 0.0$  dB; a 5.0 dB gain relative to performance using *cross-operation* CBAD processing.

### 5.3 GRLVQI Hardware Component Discrimination

Two different input sequences were considered for GRLVQI processing: TD *Statistical RF-DNA Features* and CD *Statistical CBAD Features*. GRLVQI processing enabled Dimensional Reduction Analysis (DRA) such that the original  $N_S=15880$  dimensional input TD waveform sequences  $x[n]$  were reduced to  $N_{DRA}=156$  dimensional *RF-DNA Feature Sequences* and  $N_{DRA}=10$  dimensional *CBAD Feature Sequences* based on GRLVQI feature relevance rankings.

The DRA input sequences were generated using TD waveform sequences collected from  $N_{Dev}=10$  PLC devices. For evaluating GRLVQI performance the devices were arbitrarily grouped into a set of five *authorized* devices  $\{WQ, WV, KV, OV, RG\}$  and five *rogue* devices  $\{KG, QI, ZA, ZC, ZZ\}$ . GRLVQI processing results were analyzed using ROC curves with  $EER$  providing a single measure of performance. ROC curves were used for making two assessments: 1) *Authorized Device Verification*—an assessment of how discernable the authorized devices are from each other, and 2) *Rogue Device Detection*—an assessment of how discernable a non-authorized device is from each of the authorized devices. A single benchmark criteria of  $EER_B \leq 10.0\%$  was used to evaluate the GRLVQI process for the RF-DNA and CD feature sequence inputs.

For authorized device ID verification, the  $EER_B \leq 10.0\%$  was achieved for all of the authorized devices at  $SNR=15.0$  dB using the TD RF-DNA sequences. Using the CD CBAD input sequences for authorized device ID verification, the  $EER_B \leq 10.0\%$  was achieved for three of the authorized devices at  $SNR=15.0$  dB; devices  $\{KV, WV\}$  were the exception and only achieved  $EER_B \approx 18\%$  ( $KV$ ) and  $EER_B \approx 24\%$  ( $WV$ ) at the same  $SNR$ . Rogue device detection performance met both performance benchmarks. The  $EER_B \leq 10.0\%$  benchmark achieved for all of the *Actual:Claimed* device pairs for both input sequence types at the same  $SNR$ . The generally poor performances for assessments involving device  $\{KV, WV\}$  was attributed to their CBAD features being similar to the other authorized devices  $\{KV, OV, RG\}$ .

**Performance:** With the exception of assessments involving the CBAD features for  $\{KV, WV\}$  devices and authorized device discrimination, GRLVQI processing using both TD RF-DNA and CD CBAD input sequences was effective for verifying authorized device IDs with the  $EER_B \leq 10.0\%$  benchmark achieved for  $SNR=15.0$  dB. The  $\{KV, WV\}$  device CBAD features were insufficiently distinct from each of the authorized devices. Both TD RF-DNA and CD CBAD input sequences were effective for performing *Actual:Claimed* rogue ID assessment, with the  $EER_B \leq 10.0\%$  benchmark achieved for  $SNR=15.0$  dB.

#### 5.4 Future Research Recommendations

Research results here provide proof-of-concept demonstration for employing the proposed CBAD process in many anomaly detection applications, i.e., any binary problem space where a cause-independent determination of abnormal is required. Verification-based anomaly detection was performed here using TD RF-DNA features, with Hilbert transformed sequences input to 1) the CBAD process to assess *software anomaly detection* capability, and 2) the GRLVQI process to assess *hardware component discrimination* capability. The success of demonstrations here provides opportunity for expanding verification-based approaches and several avenues of future research are recommended.

1. Alternate Signal Transforms: The analysis here focused on Hilbert transform and RF-DNA transform features derived from TD waveform responses. Actionable verification and anomaly detection information may also reside in other domains, including a) some that have been considered for other signal types and applications, e.g., 1D Spectral Domain (SD) and various 2D Wavelet, Gabor, etc., or b) some which have yet to be discovered. Features from these alternate domains, and their impact on CBAD and GRLVQI process, could be considered and may provide improvement relative to Hilbert and RF-DNA features considered here.
2. Extension to CBAD Far-Field Features: The CBAD features here were derived exclusively from near-field emissions and used primarily for verification, with some brief discussion of how classification may be implemented. A wide variety of wireless signals have been considered in related classification and verification research using far-field emission collections. Given that CBAD processing is inherently sequence agnostic, CBAD features could be easily extracted from far-field emissions to assess classification and verification. Wireless signals, particularly, present a promising avenue for future investigation given their standard-compliant, engineered waveform structure.

3. Alternate RF-DNA Region of Interest Selection and Segmentation: Currently, RF-DNA features are extracted from identically sized, evenly distributed regions within a waveform sequence. These RF-DNA features are then concatenated to form the entire RF-DNA sequence. By allowing the regions to be arbitrarily defined, the calculation of signal attributes and statistic features can be tailored to specific regions of the Intentional Radiated Emissions (IRE) or Unintentional Radiation Emissions (URE). Assuming different signal paths are used for different IRE and URE regions, use of arbitrary regions allows targeting of specific *components* within a device, offering more potential for uniquely identify and discriminating between devices.
4. Non-Binary Device Operation Assessment: Development of the binary anomaly versus normal verification-based assessment process revealed that unique waveform “shapes” can be directly attributed to device operations, e.g., the PLC execution of (*MOV*) and square-root (*SQR*) commands produced distinct emission responses. Additional research could leverage this unique operation-to-waveform response mapping to identify and extract the embedded/programmed code being executed by the device on an operation-by-operation basis. A simple implementation may include parallel matched-filtering such as commonly used for digital communication symbol estimation [72], with each parallel filter branch matched to a specific software operation response.
5. Alternate IC Devices/Near-Field Probing: Research here was based solely on emissions collected from the P80C32UFAA microcontroller on the PLC mainboard using a single near-field probe. The research could be expanded upon by considering a) emissions from an alternate IC on the PLC mainboard collected with a single near-field probe, b) emissions from the same or alternate IC on the PLC mainboard using multiple near-field probes or a near-field probe array, or, c) emissions collected simultaneously from multiple ICs on the PLC mainboard using either a single near-field probe or near-field probe array.

6. Extension to Wired Emission/Waveform Responses: As developed and demonstrated, the CBAD process is inherently sequence agnostic and can process sequences derived from any signal, system, etc., including emissions/waveforms associated with network traffic. There is ongoing SCADA field bus assessment work at AFIT and related Ethernet device work outside of AFIT [26] that may benefit from CBAD processing and which could prove valuable for identifying undesired, potentially malicious activity.
7. Extension to Environmental Effects: As developed and demonstrated, the CBAD process is focused on *software* and *hardware* anomalies based on RF emissions from IC devices. In addition to changes due to the anomalies mentioned here, factors such as temperature, device age, and humidity may also alter the collected RF emissions. Features from varied environments could be considered to evaluate the performance of the CBAD process under varying environmental conditions.

### 5.5 *Sponsor Acknowledgment*

Research sponsored in part by the Air Force Civil Engineering Center (AFCEC), Joint Base San Antonio-Lackland, TX, the RF & Microwave Systems Group, Oak Ridge National Laboratory (ORNL), Oak Ridge, TN, and Sensors Directorate, Air Force Research Laboratory (AFRL/Ry), Wright-Patterson AFB, OH.



## Bibliography

1. Abadir, M., and Reghbati, H. “Functional Testing of Semiconductor Random Access Memories,” *ACM Computer Survey*, 15:175–198 (Sep 1983).
2. Agrawal, D., S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar. “Trojan Detection using IC Fingerprinting.” *Security and Privacy, 2007. SP '07. IEEE Symposium on*. 296 –310. May 2007.
3. Baranski, W., A. Wytyczak-partyka, and T. Walkowiak. *Computational Complexity Reduction in PCA-based Face Recognition*. Technical Report, Institute of Computer Engineering, Control and Robotics, Wroclaw University of Technology, 2007.
4. Bureau of Industry and Security, Office of Technology Evaluation. *Defense Industrial Base Assessment: Counterfeit Electronics*. Technical Report, U.S. Department of Commerce, 2010.
5. Bush, G. *Homeland Security Presidential Directive 7*. Technical Report, The White House, Washington DC: U.S. Government, Dec 2003.
6. Chouchane, A., S. Rekhis, and N. Boudriga. “Defending Against Rogue Base Station Attacks Using Wavelet Based Fingerprinting.” *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on*. 523 –530. May 2009.
7. Cisco, “OSI Reference Model,” Cisco Certified Network Associate (CCNA) Guru Website, [www.ccnaguru.com/osi-reference-model.html](http://www.ccnaguru.com/osi-reference-model.html), May 2009.
8. CMD CTR USSTRATCOM(UC), “Subject: Suspension of Removable Flash Media,” 2008.
9. Cobb, W. *Exploitation of Unintentional Information Leakage from Integrated Circuits*. Dissertation, Air Force Institute of Technology, Dec 2011.
10. Cobb, W., E. Garcia, M. Temple, R. Baldwin, and Y. Kim. “Physical layer identification of embedded devices using RF-DNA fingerprinting.” *Military Communications Conference, 2010 - MILCOM 2010*. 2168 –2173. Nov 2010.
11. Cobb, W., E. Laspe, R. Baldwin, M. Temple, and Y. Kim. “Intrinsic Physical-Layer Authentication of Integrated Circuits,” *Information Forensics and Security, IEEE Transactions on*, 7:11 (Feb 2012).
12. CrySyS. *Duqu: A Stuxnet-like Malware Found in the Wild*. Technical Report, Budapest University of Technology and Economics Department of Telecommunications, 2011.

13. CrySyS. *sKyWIper (a.k.a. Flame a.k.a. Flamer): A Complex Malware for Targeted Attacks*. Technical Report, Budapest University of Technology and Economics Department of Telecommunications, May 2012.
14. Danev, B., and S. Capkun. "Transient-Based Identification of Wireless Sensor Nodes." *8th ACM/IEEE Int'l Conf on Information Processing in Sensor Networks (IPSN09)*. Apr 2009.
15. Danev, B., H. Luecken, S. Capkun, and K. Defrawy. "Attacks on Physical-layer Identification." *Third ACM conference on Wireless network security, WiSec 2010*. 89–98. Mar 2010.
16. Danev, B., T. Heydt-Benjamin, and S. Capkun. "Physical-layer Identification of RFID Devices." *18th Conf on USENIX Security Symposium*. SSYM'09. 199–214. 2009.
17. DARPA, "TRUST for Integrated Circuits Proposal Solicitation: BAA06-40," 2006.
18. DeJean, G., and D. Kirovski. "RF-DNA: Radio-Frequency Certificates of Authenticity." *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*. 346–363. 2007.
19. Desmond, L., C. Yuan, T. Pheng, and R. Lee. "Identifying Unique Devices Through Wireless Fingerprinting." *1st ACM conference on Wireless Network Security*. WiSec '08. 46–55. N: ACM, 2008.
20. Downie, J., and J. Walkup. "Optimal Correlation Filters for Images with Signal-dependent Noise," *Journal of the Optical Society of America A*, 11(5):1599–1609 (May 1994).
21. Dubendorfer, C., B. Ramsey, and M. Temple. "An RF-DNA Verification Process for ZigBee Networks." *Military Communications Conference, 2012 - MIL-COM 2012*. 1–6. 2012.
22. Duda, R., P. Hart, and D. Stork. *Pattern Classification* (2nd Edition). New York: John Wiley & Sons, 2001.
23. Dudeczyk, J., and M. Wnuk. "The Utilization of Unintentional Radiation for Identification of the Radiation Source." Oct 2004.
24. Dudeczyk, J., J. Matuszewski, and M. Wnuk. "Applying the Radiated Emission to the Specific Emitter Identification." May 2004.
25. Ellis, K., and N. Serinken. "Characteristics of Radio Transmitter Fingerprints," *Radio Science*, 36(4):585–597 (2001).
26. Gerdes, R., M. Mina, S. Russell, and T. Daniels. "Physical-Layer Identification of Wired Ethernet Devices," *Information Forensics and Security, IEEE Transactions on*, 7(4):1339–1353 (2012).

27. Gimelshteyn, M. *Classifying Commercial Receiver Emissions Using Fisher Discriminant Analysis*. MS thesis, AFIT, 2007.
28. González, C., and J. Reed. “Detecting unauthorized software execution in SDR using power fingerprinting.” *Military Communications Conference, 2010 - MILCOM 2010*. 2211–2216. Nov 2010.
29. González, C., and J. Reed. “Power fingerprinting in SDR integrity assessment for security and regulatory compliance,” *Analog Integr. Circuits Signal Process.*, 69(2-3):307–327 (Dec 2011).
30. Hahn, S. “Comments on “A Tabulation of Hilbert Transforms for Electrical Engineers”,” *Communications, IEEE Transactions on*, 44(7):768 (1996).
31. Hahn, S. *Hilbert transforms in signal processing*. Artech House signal processing library, Artech House, 1996.
32. Hahn, S. *The Transforms and Applications Handbook* (3 Edition). Boca Raton, FL: CRC Press, Jan 2010.
33. Hale, G. *Stuxnet Effect: Iran Still Reeling*. Technical Report, August 2011.
34. Hall, E., J. Budinger, R. Dimond, J. Wilson, and R. Apaza. “Aeronautical Mobile Airport Communications System Development Status.” *Integrated Communications Navigation and Surveillance Conference (ICNS), 2010*. A4–1–A4–15. may 2010.
35. Hall, J., M. Barveau, and E. Kranakis. “Detection of Transient in Radio Frequency Fingerprinting using Signal Phase.” *Proceedings of IASTED International Conference on Wireless and Optical Communications (WOC '03)*. 2003.
36. Hall, J., M. Barveau, and E. Kranakis. “Radio Frequency Fingerprinting for Intrusion Detection in Wireless Networks,” *IEEE Transactions on Dependable and Secure Computing*, 1–1–35 (2005).
37. Hall, J., M. Barveau, and E. Kranakis. “Detecting Rogue Devices in Bluetooth Networks Using Radio Frequency Fingerprinting.” *Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN '06)*. Oct 2006.
38. Hall, J. “Enhancing Intrusion Detection in Wireless Networks using Radio Frequency Fingerprinting.” *In Proceedings of the 3rd IASTED International Conference on Communications, Internet and Information Technology (CIIT)*. 201–206. Kranakis, 2004.
39. Harmer, P., and M. Temple. “An improved LFS Engine for Physical Layer Security Augmentation in Cognitive Networks.” *Computing, Networking and Communications (ICNC), 2013 International Conference on*. 719–723. 2013.

40. Harmer, P., M. Temple, M. Buckner, and E. Farquahar. "Using Differential Evolution to Optimize 'Learning from Signals' and Enhance Network Security." *Proceedings of the 13th Annual Conference on Genetic and Evolutionary Computation*. GECCO '11. 1811–1818. New York, NY, USA: ACM, 2011.
41. Harmer, P., M. Temple, M. Buckner, and E. Farquhar. "4G Security Using Physical Layer RF-DNA with DE-Optimized LFS Classification.," *JCM*, 6(9):671–681 (2011).
42. Harmer, P., M. Williams, and M. Temple. "Using DE-Optimized LFS Processing to Enhance 4G Communication Security." *Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on*. 1–8. Aug 2011.
43. Ho, T., and M. Basu. "Complexity Measures of Supervised Classification Problems," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 24(3):289–300 (Mar 2002).
44. Hodson, H., "Hackers Accessed City Infrastructure via SCADA," Nov 2011.
45. ICS-CERT. *ICS-CERT Homepage*. Technical Report.
46. ICS-CERT. *ICS Monitor*. Technical Report, US Department of Homeland Security, 2013.
47. IEEE. *IEEE Std 802.15.1-2005*. Technical Report, IEEE, 2005.
48. Jain, A., A. Ross, A., and S. Prabhakar. "An Introduction to Biometric Recognition," *Circuits and Systems for Video Technology, IEEE Transactions on*, 14(1):4–20 (Jan 2004).
49. Jana, S., and S. Kasera. "Wireless Device Identification with Radiometric Signatures." *ACM 14th Int'l Conf on Mobile Computing and Networking (MOBICOM08)*. Sep 2008.
50. Kak, S. *The Discrete Finite Hilbert Transform*. Technical Report, Indian Institute of Technology, Sep 1975.
51. Kay, S. *Intuitive Probability and Random Processes using MATLAB*. Springer, 2005.
52. Keller, W., and B. Pathak. *Integrated Circuit with Electromagnetic Energy Anomaly Detection and Processing*. Technical Report 20120223403, 2012.
53. Kim, L., and J. Villasenor. "A System-On-Chip Bus Architecture for Thwarting Integrated Circuit Trojan Horses," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, 19(10):1921–1926 (Oct 2011).
54. Kim, Y., V. Agrawal, and K. Saluja. "Multiple Faults: Modeling, Simulation and Test." *Design Automation Conference, 2002. Proceedings of ASP-DAC*

2002. *7th Asia and South Pacific and the 15th International Conference on VLSI Design. Proceedings.* 592–597. 2002.
55. Kim, Y., V. Agrawal, and K. Saluja. “Combinational Automatic Test Pattern Generation for Acyclic Sequential Circuits,” *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, 24(6):948–956 (Jun 2005).
  56. Klein, R. *Application of Dual-Tree Complex Wavelet Transforms to Burst Detection and RF Fingerprint Classification*. PhD dissertation, Air Force Institute of Technology, Sep 2009.
  57. Klein, R., M. Temple, and M. Mendenhall. “Application of Wavelet-Based RF Fingerprinting to Enhance Wireless Network Security,” *Jour of Communications and Networks*, 11(6):544; 12; 114–555 (Dec 2009).
  58. Klein, R., M. Temple, M. Mendenhall, and D. Reising. “Sensitivity Analysis of Burst Detection and RF Fingerprinting Classification Performance.” *IEEE International Conference on Communications, 2009. ICC '09.* 1–5. Jun 2009.
  59. Kuciapinski, K., M. Temple, and R. Klein. “ANOVA-based RF DNA analysis: Identifying Significant Parameters for Device Classification.” *Wireless Information Networks and Systems (WINSYS), Proceedings of the 2010 International Conference on*. 1–6. Jul 2010.
  60. MacKenzie, H. *Shamoon Malware and SCADA Security What are the Impacts?*. Technical Report, Tofino Security, Sep 2012.
  61. Mateti, P. *Hacking Techniques in Wireless Networks* (1 edition Edition), 3. The Handbook of Information Security, chapter 138, 991–1001. Hoboken, NJ: John Wiley, 2005.
  62. Mathworks, “Discrete-time Analytic Signal Using Hilbert Transform.” Website.
  63. McAfee Labs. *2013 Threats Predictions*. Technical Report, McAfee, 2012.
  64. McMinn, L., and J. Butts. “A Firmware Verification Tool for Programmable Logic Controllers.” *Critical Infrastructure Protection VI VI*, edited by J. Butts and S. Sheno. Springer, Heidelberg, 2012.
  65. NASA. *EEE Parts Bulletin*. Technical Report, NASA, May/Jun 2011.
  66. Obama, B. *Executive Order : Improving Critical Infrastructure Cybersecurity*. Technical Report, The White House, Washington DC: U.S. Government, Feb 2013.
  67. Oppenheim, A., and R. Schaffer. *Discrete-Time Signal Processing* (3rd Edition). Upper Saddle River, NJ, USA: Prentice Hall Press, 2009.

68. Paar, C., T. Eisenbarth, M. Kasper, T. Kasper, and A. Moradi. "KeeLoq and Side-Channel Analysis-Evolution of an Attack." *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2009 Workshop on*. 65–69. Sep 2009.
69. Paul, J., S. Stone, Y. Kim, R. Bennington. "A Method and FPGA Architecture for Real-Time Polymorphic Reconfiguration." *Field-Programmable Technology, 2007. ICFPT 2007. International Conference on*. 65–71. Dec 2007.
70. Porter, R., S. Stone, Y. Kim, J. McDonald, and L. Starman. "Dynamic Polymorphic Reconfiguration for Anti-tamper Circuits." *Field Programmable Logic and Applications, 2009. FPL 2009. International Conference on*. 493–497. Sep 2009.
71. Potamianos, A., R. Potamianos, P. Maragos, and P. Maragos. *A Comparison of the Energy Operator and the Hilbert Transform Approach to Signal and Speech Demodulation*. Technical Report, School of Electrical & Computer Engineering, Georgia Institute of Technology, 1994.
72. Proakis, J. *Digital Communications*. McGraw-Hill, 2000.
73. Rahman, M., and H. Imai. "Security in Wireless Communication," *Wireless Personal Communications*, 22:213–228 (2002). 10.1023/A:1019968506856.
74. Ramsey, B., M. Temple, and B. Mullins. "PHY Foundation for Multi-Factor ZigBee Node Authentication." *Global Communications Conference (GLOBECOM), 2012 IEEE*. 795–800. 2012.
75. Reising, D., "Classifying Emissions from Global System for Mobile (GSM) Communication Devices Using Radio Frequency (RF) Fingerprints," 2009.
76. Reising, D. *Exploitation of RF-DNA for Device Classification and Verification Using GRLVQI Processing*. PhD dissertation, Air Force Institute of Technology, 2012.
77. Reising, D., and M. Temple. "WiMAX Mobile Subscriber Verification using Gabor-Based RF-DNA Fingerprints." *Communications (ICC), 2012 IEEE International Conference on*. 1005–1010. 2012.
78. Reising, D., M. Temple, and J. Jackson. "Dimensionally Efficient ID Verification of OFDM-Based Devices Using GRLVQI Processing," *Journal on Selected Areas in Communications, IEEE* (2012, UNDER REVIEW).
79. Reising, D., M. Temple, and M. Mendenhall. "Improved Wireless Security for GMSK Based Devices Using RF Fingerprinting," *Int. J. Electron. Secur. Digit. Forensic*, 3:41–59 (Mar 2010).
80. Reising, D., M. Temple, and M. Mendenhall. "Improving Intra-Cellular Security Using Air Monitoring with RF Fingerprints." *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*. 1–6. Apr 2010.

81. Reising, D., M. Temple, and M. Oxley. "Gabor-based RF-DNA Fingerprinting for Classifying 802.16e WiMAX Mobile Subscribers." *Computing, Networking and Communications (ICNC), 2012 International Conference on*. 7 –13. Feb 2012.
82. S. Das, K. Kant, N. Zhang. *Handbook on Securing Cyber-Physical Critical Infrastructure..* Kaufmann, M, 2012.
83. Scarfone, K., and P. Mell, "Guide to Intrusion Detection and Prevention Systems," Feb 2007.
84. Shaw, W. *Cybersecurity for SCADA Systems* (1 Edition). Tulsa, OK: PennWell Corporation, 2006.
85. Sklar, B. *Digital Communications: Fundamentals and Applications*. Prentice Hall, 2009.
86. Stone, S., and M. Temple. "RF-Based Anomaly Detection for PLCs." *Sixth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection*. 2012.
87. Stone, S., and M. Temple. "RF-Based Anomaly Detection For PLCs in Critical Infrastructure Applications," *International Journal of Critical Infrastructure Protection*, 5(2):11–33 (Jul 2012).
88. Stone, S., and M. Temple. "Detecting Anomalous SCADA Operation Using RF-Based Hilbert Transforms," *International Journal of Critical Infrastructure Protection*, 5(2):11–33 (Jul 2013).
89. Stone, S., and M. Temple, and R. Baldwin. "RF-Based PLC IC Design Verification." *2012 DMSMS & Stand Conf. (DMSMS12)*. Nov 2012.
90. Stone, S., R. Porter, Y. Kim, and J. Paul. "A Dynamically Reconfigurable Field Programmable Gate Array Hardware Foundation for Security Applications." *ICECE Technology, 2008. FPT 2008. International Conference on*. 305 –308. Dec 2008.
91. Suski, W., M. Temple, M. Mendenhall, and R. Mills. "Radio Frequency Fingerprinting Commercial Communication Devices to Enhance Electronic Security," *Int. J. Electron. Secur. Digit. Forensic*, 1:301–322 (Oct 2008).
92. Suski, W., M. Temple, M. Mendenhall, and R. Mills. "Using Spectral Fingerprints to Improve Wireless Network Security." *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*. 1 –5. Dec 2008.
93. Symantec Security Response. *W32.Duqu: The Precursor to the Next Stuxnet*. Technical Report, Symantec, 2011.
94. Symantec Security Response. *W32.Stuxnet Dossier*. Technical Report, Symantec, 2011.

95. Tsang, R. *Cyberthreats, Vulnerabilities and Attacks on SCADA Networks*. Technical Report, Goldman School of Public Policy, 2009.
96. Ureten, O., and N. Serinken. “Detection of Radio Transmitter Turn-On Transients,” *Electronics Letters*, 35(23):1996–1997 (Nov 1999).
97. Ureten, O., and N. Serinken. “Wireless Security Through RF fingerprinting,” *Electrical and Computer Engineering, Canadian Journal of*, 32(1):27–33 (Winter 2007).
98. U.S. Congress. *USA PATRIOT ACT of 2001 (U.S. H.R. 3162, Public Law 107-56)*. Technical Report, Washington DC: U.S. Government, Oct 2001.
99. USAF AFCERT. *AFCERT Operations Metrics*. Metrics, San Antonio, TX: USAF, Dec 2011.
100. Watley, T., “Memorandum for LDRD Proposal Review Committee,” Jun 2012.
101. Wetula, A. “A Hilbert Transform Based Algorithm for Detection of a Complex Envelope of a Power Grid Signals an Implementation,” *Electrical Power Quality and Utilisation, Journal*, XIV(2):13–18 (2008).
102. Williams, M., M. Temple, and D. Reising. “Augmenting Bit-Level Network Security Using Physical Layer RF-DNA Fingerprinting.” *GLOBECOM 2010, 2010 IEEE Global Telecommunications Conference*. 1–6. Dec 2010.
103. Williams, M., S. Munns, M. Temple, and M. Mendenhall. “RF-DNA Fingerprinting for Airport WiMax Communications Security.” *Network and System Security (NSS), 2010 4th International Conference on*. 32–39. Sep 2010.
104. Wright, J. *Detecting Wireless LAN MAC Address Spoofing*. Technical Paper, Johnson & Wales University, 2003.
105. Zetter, K. *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*. Technical Report, Jul 2011.
106. Zimmermann, H. “OSI Reference Model—The ISO Model of Architecture for Open Systems Interconnection,” *Communications, IEEE Transactions on*, 28(4):425–432 (Apr 1980).



REPORT DOCUMENTATION PAGE					Form Approved OMB No. 0704-0188	
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. <b>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</b></p>						
1. REPORT DATE (DD-MM-YYYY)		2. REPORT TYPE		3. DATES COVERED (From — To)		
12-09-2013		Doctoral Dissertation		Sep 2010-Sep 2013		
4. TITLE AND SUBTITLE  Radio Frequency Based Programmable Logic Controller Anomaly Detection				5a. CONTRACT NUMBER		
				5b. GRANT NUMBER		
				5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S)  Stone, Samuel J., Capt, USAF				5d. PROJECT NUMBER		
				5e. TASK NUMBER		
				5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way WPAFB OH 45433-7765 DSN: 785-3636				8. PERFORMING ORGANIZATION REPORT NUMBER  AFIT-ENG-DS-13-S-05		
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Research Laboratory, AFMC Attn: AFRL/RV (Dr. Vasu Chakravarthy) 2241 Avionics Circle, Bldg 620 WPAFB OH 45433-7734 (937)528-8269 Vasu.Chakravarthy@wpafb.af.mil				10. SPONSOR/MONITOR'S ACRONYM(S)  AFRL/RV		
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION / AVAILABILITY STATEMENT  DISTRIBUTION STATEMENT A. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED						
13. SUPPLEMENTARY NOTES						
14. ABSTRACT This dissertation introduces research activity and results for development and demonstration of a verification-based Programmable Logic Controller (PLC) anomaly detection approach that supports 1) <i>software anomaly detection</i> and 2) <i>hardware anomaly detection</i> . The Correlation Based Anomaly Detection (CBAD) process developed here is used to detect <i>software-based</i> anomalies, while the Generalized Relevance Learning Vector Quantized-Improved (GRLVQI) process previously established is used to detect <i>hardware-based</i> anomalies. A benchmark of $EER \leq 10.0\%$ is used to measure performance for both <i>hardware</i> and <i>software</i> anomaly detection. The CBAD process using Hilbert transformed Time Domain (TD) input sequences met the benchmark of $EER_B \leq 10.0\%$ at $SNR = 0.0$ dB. Untransformed TD sequences and RF-DNA sequences, when used for the CBAD process, did not meet the performance benchmark. The GRLVQI process using TD feature and Correlation Domain (CD) input sequences met benchmark of $EER_B \leq 10.0\%$ at $SNR = 15.0$ dB. At $SNR = 15.0$ dB an average $EER \approx 1.3\%$ was achieved for TD sequences as compared to an average $EER \approx 1.6\%$ for the CD sequences. While the $EER$ value for TD sequences is 0.3% lower than CD sequences, the TD sequence has nearly 16 times the number of elements as the CD sequence and a correspondingly greater amount of computational resources would be required in an operational implementation.						
15. SUBJECT TERMS  RF-DNA, RF Fingerprinting, GRLVQI, SCADA, ICS, Critical Infrastructure, Verification, Cyber Security						
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON	
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Michael A. Temple	
U	U	U	UU	131	19b. TELEPHONE NUMBER (include area code) (937) 255-3636,x4279, michael.temple@afit.edu	